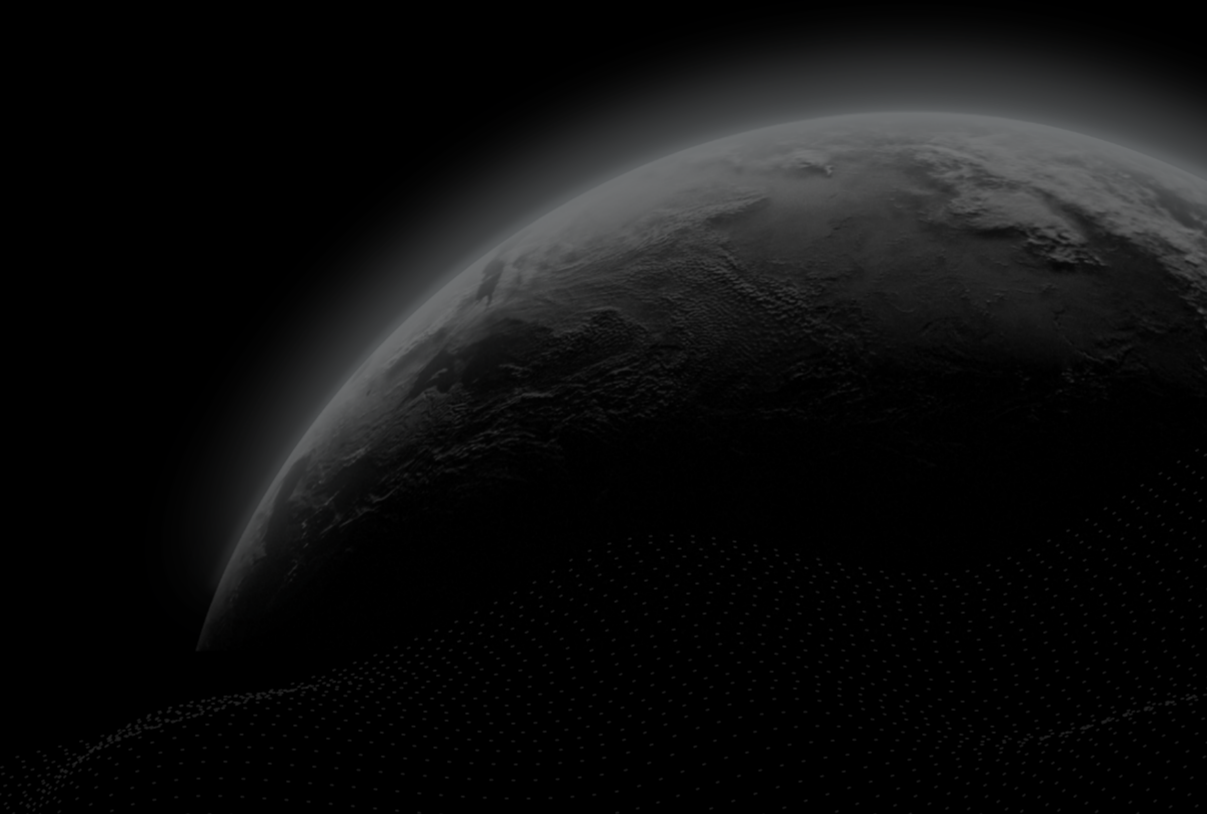
Security Assessment

Iskra - Audit for Token (Part 1)

CertiK Verified on May 17th, 2023



CertiK Verified on May 17th, 2023

Iskra - Audit for Token (Part 1)

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

Executive Summary

TYPES
Service

ECOSYSTEM
Ethereum (ETH)

METHODS
Formal Verification, Manual Review, Static Analysis

LANGUAGE
Solidity

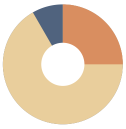
TIMELINE
Delivered on 05/17/2023

KEY COMPONENTS
N/A

CODEBASE
https://github.com/iskraworld/
...View All

COMMITS
9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665
b13f48ae98e7d814ba45bd4a3066ebcf0948478c
...View All

Vulnerability Summary



Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved
12	5	0	1	6	0	0

🟥	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.
🟧	3	Major	3 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.
🟨	0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
🟨	8	Minor	5 Resolved, 1 Partially Resolved, 2 Acknowledged	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.
🟦	1	Informational	1 Acknowledged	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 | ISKRA - AUDIT FOR TOKEN (PART 1)

CODEBASE | ISKRA - AUDIT FOR TOKEN (PART 1)

Repository

https://github.com/iskraworld/

Commit

9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665

b13f48ae98e7d814ba45bd4a3066ebcf0948478c

AUDIT SCOPE | ISKRA - AUDIT FOR TOKEN (PART 1)

5 files audited ● 5 files with Acknowledged findings

ID	File	SHA256 Checksum
● MTE	contracts/token/ERC1155/MultiToken.sol	edc535277fdc77b1457e45b46a4335541e1234b8af5ecf83f89d995e5676b845
● GTE	contracts/token/ERC20/GameToken.sol	831239d6109dad00e3d85d8f73f5570a76fa255a12a874e980a1972e1771d87f
● UTE	contracts/token/ERC20/UtilityToken.sol	fe6c098fb0ef381b973241a3ac4281dc227db0d0fe38762f03dba08b0a55c7af
● INF	contracts/token/ERC721/ItemNFT.sol	a5af9936f6e6078657584123040213f7c41beb380ca41bf3b6cbf4d880896dd2
● VET	contracts/vesting/Vesting.sol	3d3b0165b8ebd5da308bda5014c34623164ab1c08c2588a5d4d3b2f5d6eb1f7c

APPROACH & METHODS | ISKRA - AUDIT FOR TOKEN (PART 1)

This report has been prepared for Iskra to discover issues and vulnerabilities in the source code of the Iskra - Audit for Token (Part 1) 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.

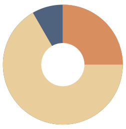
The auditing process pays special attention to the following considerations:

- 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:

- 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.

FINDINGS | ISKRA - AUDIT FOR TOKEN (PART 1)



12	0	3	0	8	1
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Iskra - Audit for Token (Part 1). Through this audit, we have uncovered 12 issues ranging from different severity levels. Utilizing the techniques of Static Analysis & Manual Review to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
CON-01	**Centralization Related Risks**	**Centralization / Privilege**	**Major**	● **Acknowledged**
GTE-01	**Initial Token Distribution**	**Centralization / Privilege**	**Major**	● **Acknowledged**
VET-01	**Centralized Control Of Contract Upgrade**	**Centralization / Privilege**	**Major**	● **Acknowledged**
INF-03	Batchminting Does Not Prevent Overflow	Volatile Code	Minor	● Acknowledged
VET-04	Unprotected Initializer	Coding Style	Minor	● Resolved
VET-05	Unchecked ERC-20 `transfer()` / `transferFrom()` Call	Volatile Code	Minor	● Resolved
VET-06	Missing Zero Address Validation	Volatile Code	Minor	● Resolved
VET-07	Check Effect Interaction Pattern Violated	Volatile Code	Minor	● Partially Resolved
VET-10	Third Party Dependency	Volatile Code	Minor	● Acknowledged
VET-11	Incompatibility With Deflationary Tokens	Volatile Code	Minor	● Resolved

ID	Title	Category	Severity	Status
VET-12	Missing Input Validation On `_reclaimer`	Control Flow, Logical Issue	Minor	● Resolved
VET-02	Inaccurate Transfer Amount	Mathematical Operations, Logical Issue	Informational	● Acknowledged

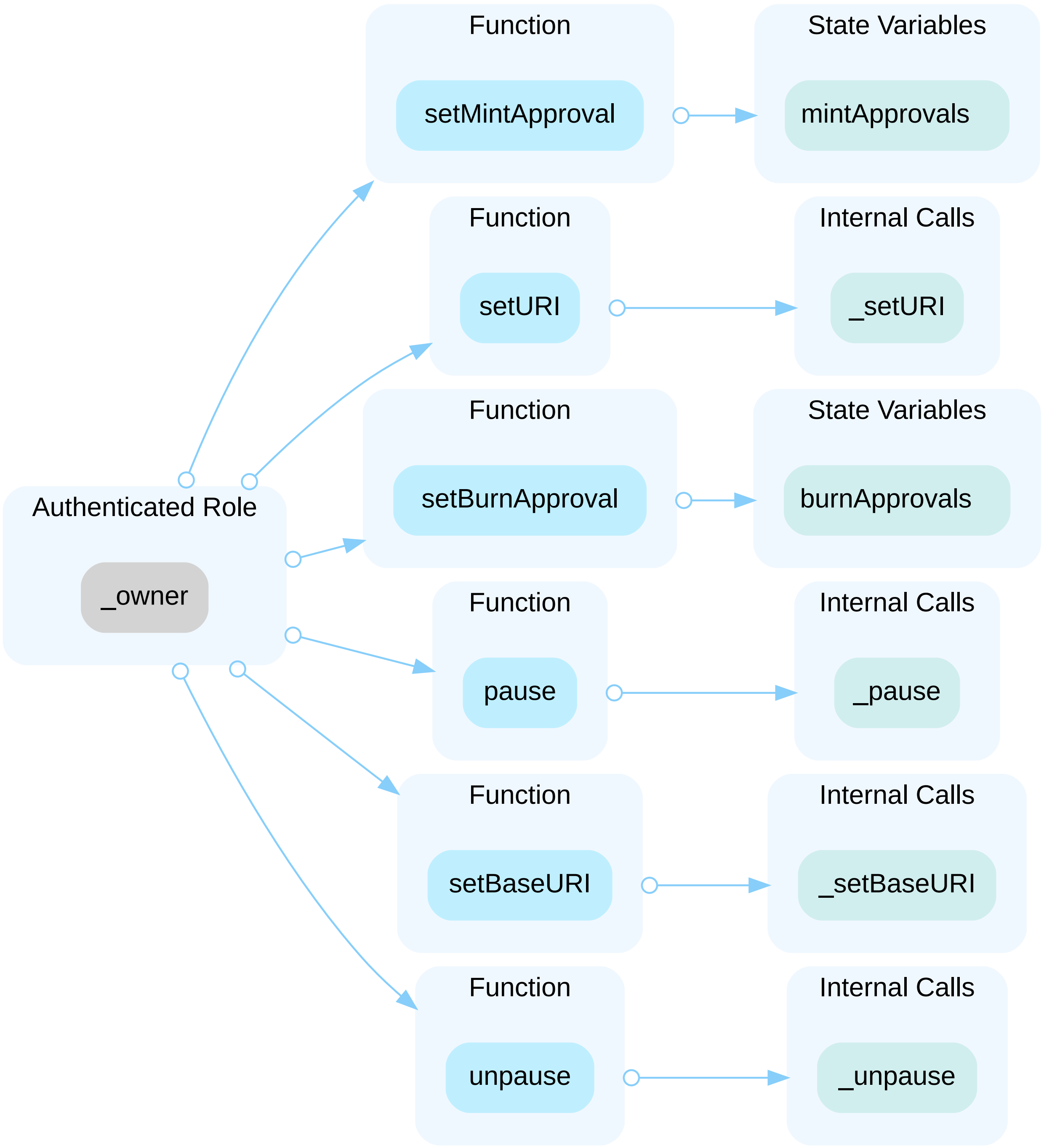
CON-01 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**contracts/token/ERC1155/MultiToken.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 60, 64, 94, 98, 102, 112; contracts/token/ERC20/UtilityToken.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 56, 67, 74, 78, 82; contracts/token/ERC721/ItemNFT.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 101, 110, 115, 135; contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 58, 119, 138, 158, 179**	● **Acknowledged**

Description

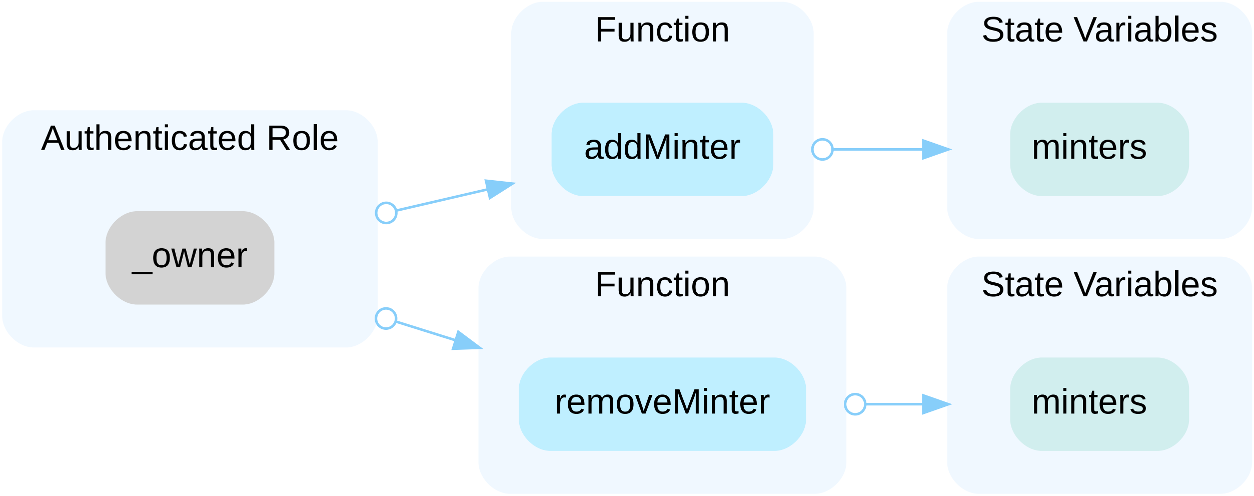
In the contract `MultiToken` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and:

- transfer the ownership to an address they control;
- change the URI;
- pause or unpause the contract (if `MultiToken` is deployed as pausable);
- grant or revoke the capacity to mint tokens from any address;
- grant or revoke the capacity to burn tokens from any address (if `MultiToken` is deployed as pausable);



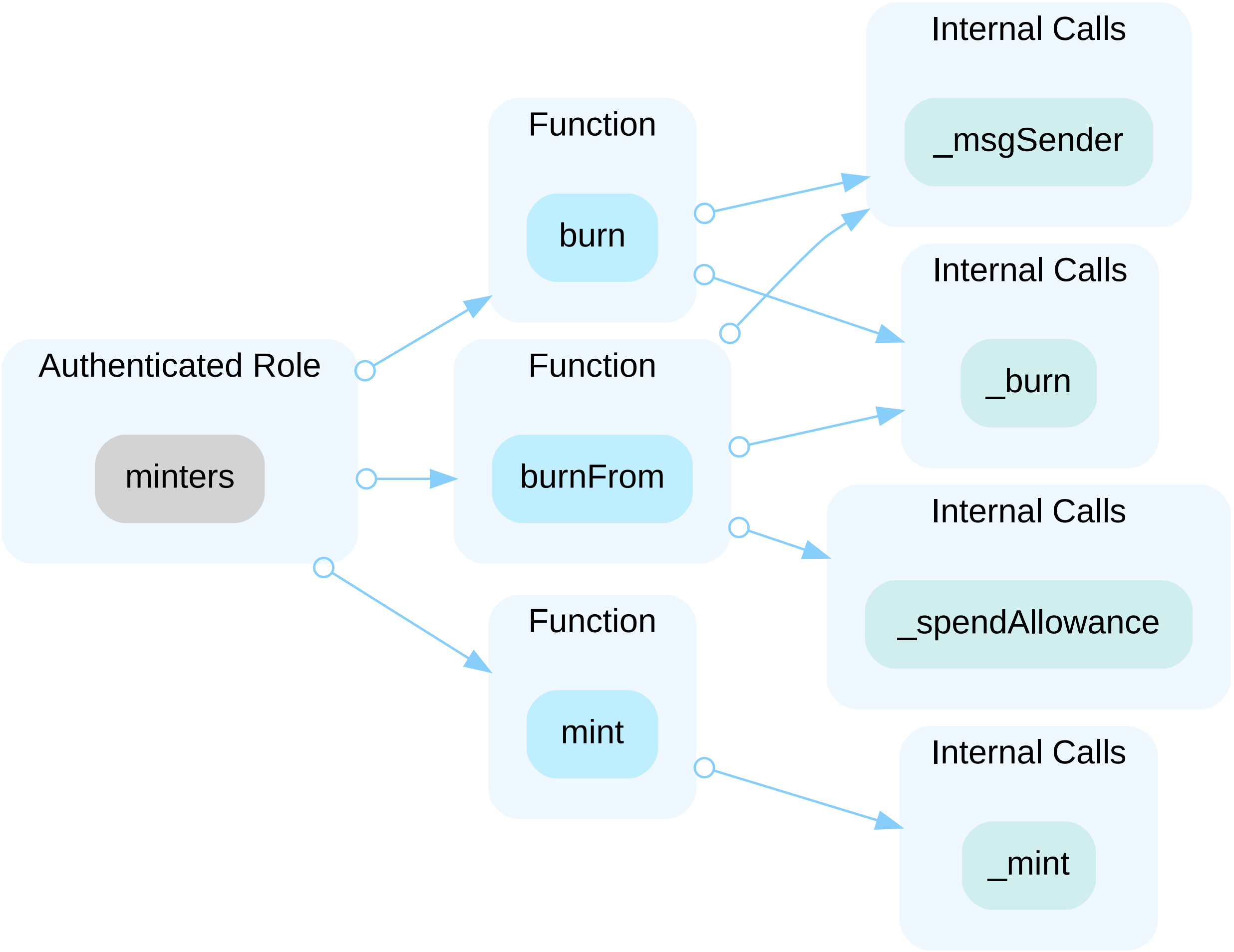
In the contract `UtilityToken` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and:

- transfer ownership to an address they control;
- grant or revoke the minter role from any address.



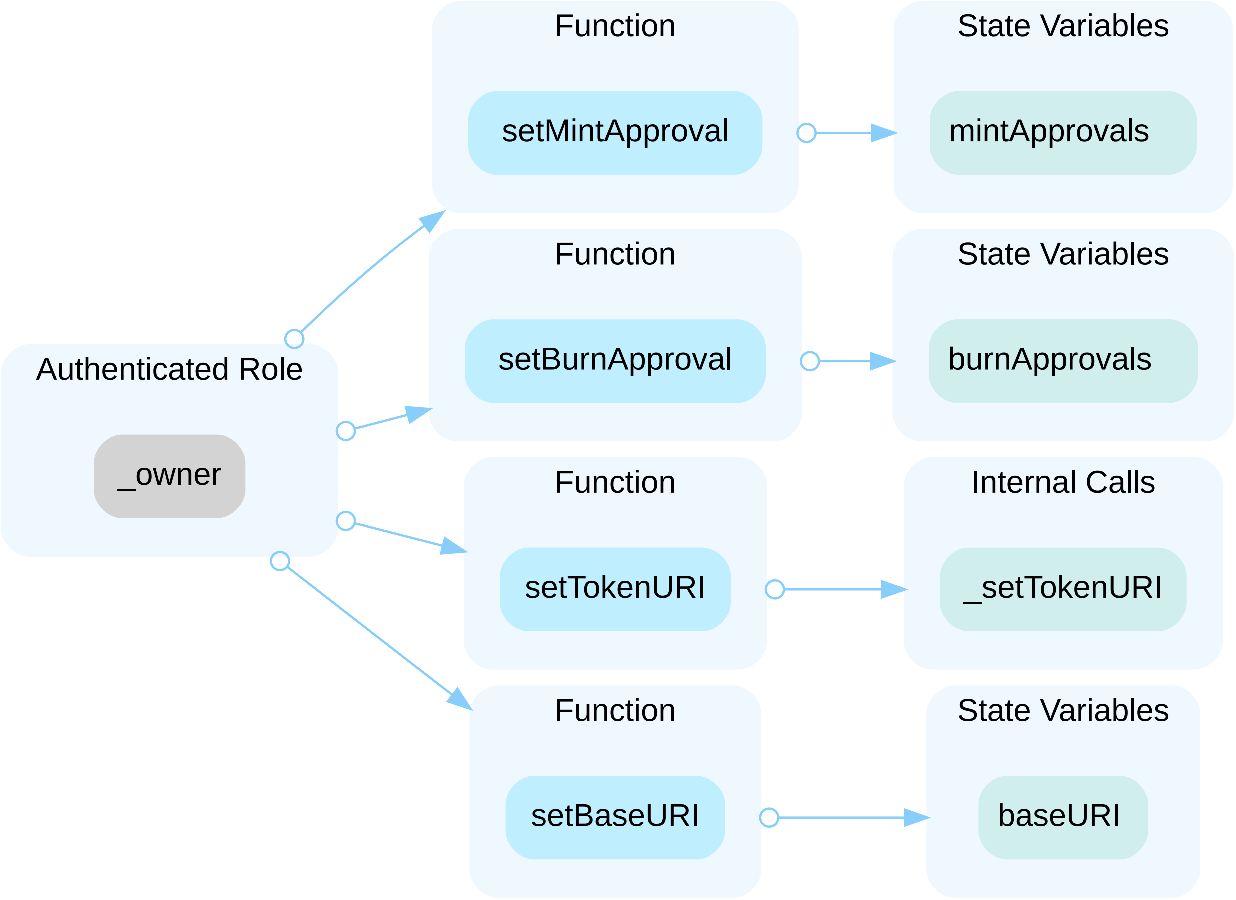
In the contract `UtilityToken` the role `minters` has authority over the functions shown in the diagram below. Any compromise to the `minters` account may allow the hacker to take advantage of this authority and :

- mint any amount of tokens to any address;
- burn tokens they own or are approved to handle.



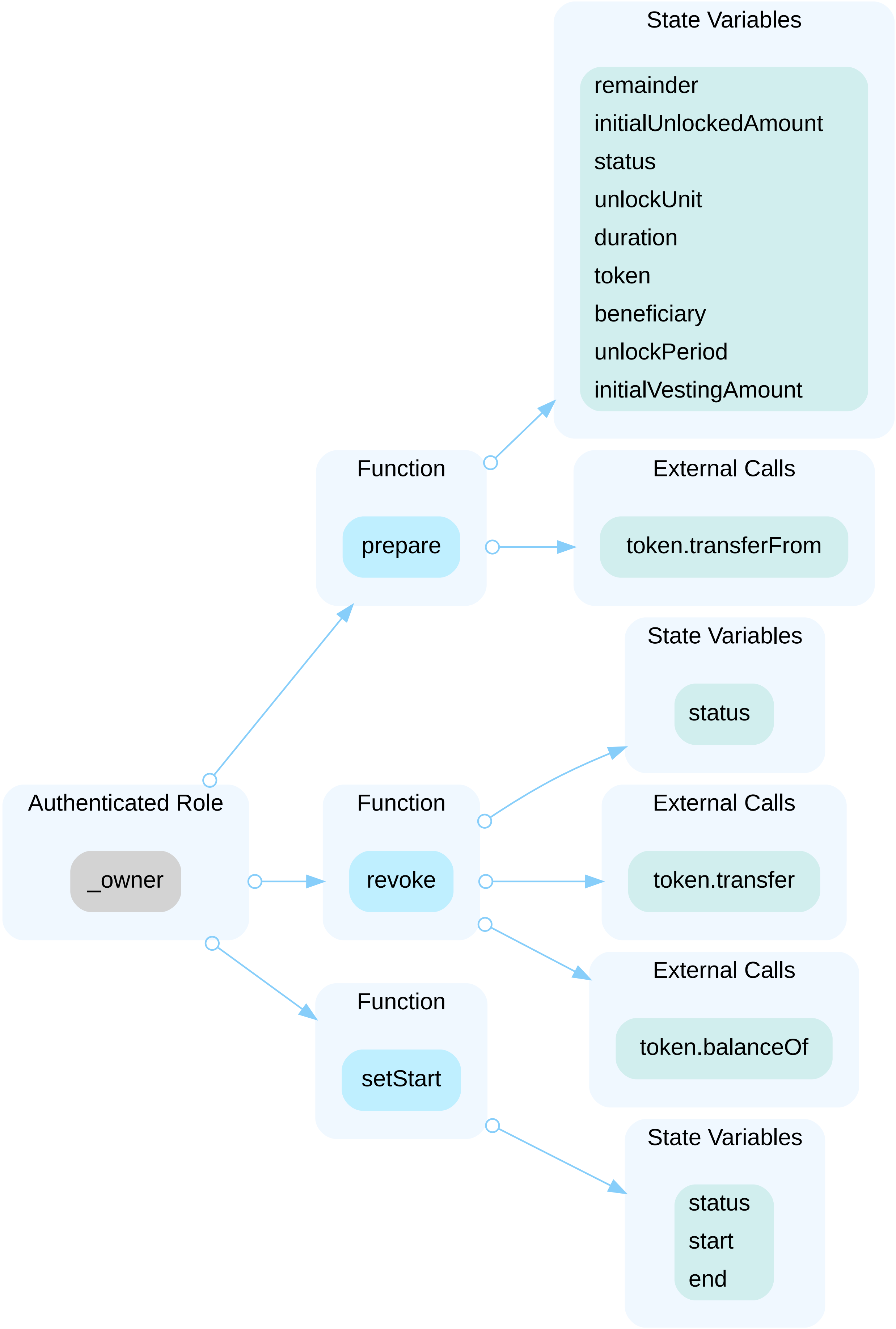
In the contract `ItemNFT` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and :

- grant or revoke the capacity to mint tokens to any address;
- grant or revoke the capacity to burn tokens to any address (if the contract has been deployed as burnable);
- change the URI;



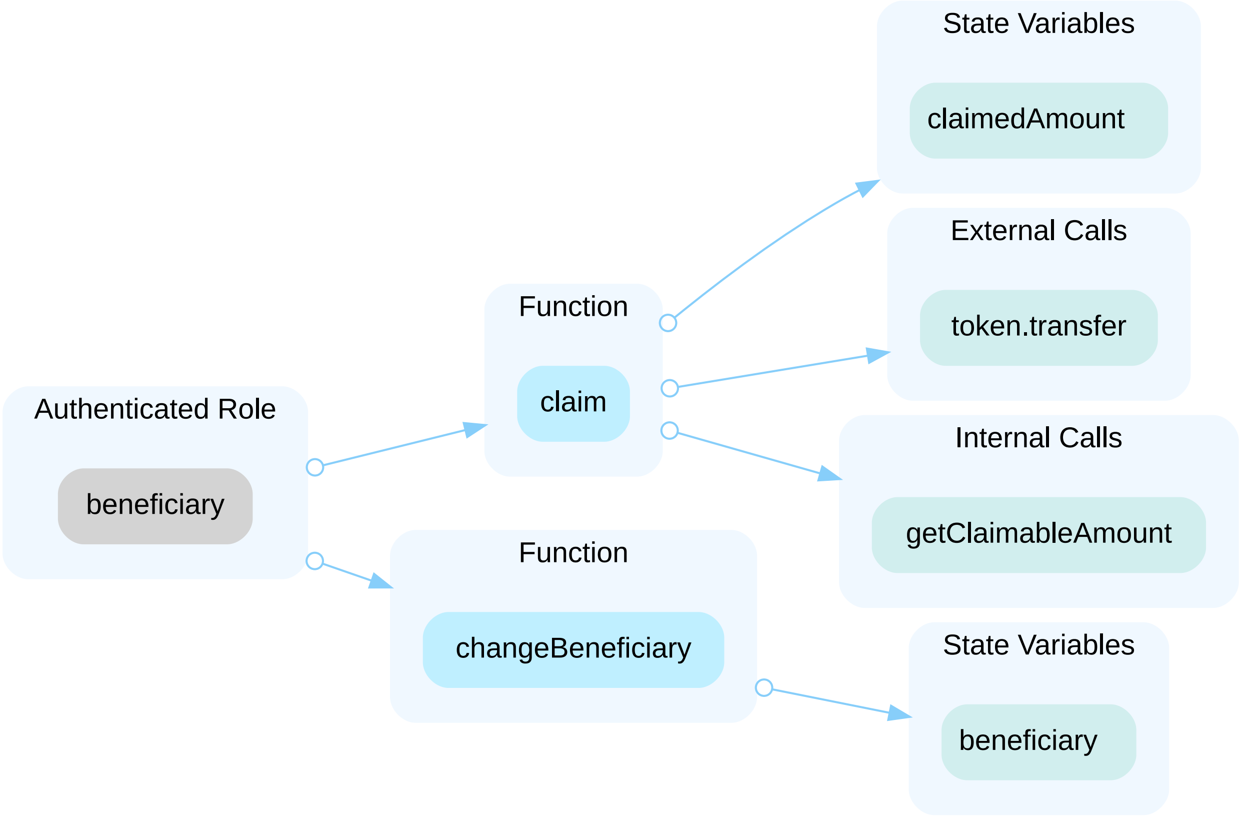
In the contract `Vesting` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and:

- transfer the ownership to an address they control;
- prepare a new vesting;
- set the start of a vesting;
- revoke the vesting and send the tokens to an address they control.


State Variables
remainder
initialUnlockedAmount
status
unlockUnit
duration
token
beneficiary
unlockPeriod
initialVestingAmount
Function
prepare
External Calls
token.transferFrom
State Variables
status
Authenticated Role
_owner
Function
revoke
External Calls
token.transfer
External Calls
token.balanceOf
Function
setStart
State Variables
status
start
end

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

- change the beneficiary address to an address they control;
- claim tokens vested;



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

[CertiK]`: The team acknowledged the finding but decide to remain unchanged.

GTE-01 | INITIAL TOKEN DISTRIBUTION

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**contracts/token/ERC20/GameToken.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 30**	● **Acknowledged**

Description

All tokens are sent to the contract deployer when deploying the contract. This is a potential centralization risk as the deployer can distribute tokens without the consensus of the community.

Recommendation

We recommend transparency through providing a breakdown of the intended initial token distribution in a public location. We also recommend the team make an effort to restrict the access of the corresponding private key.

Alleviation

[CertiK]`: The team acknowledged the finding but decide to remain unchanged.

VET-01 | CENTRALIZED CONTROL OF CONTRACT UPGRADE

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 10**	● **Acknowledged**

Description

`Vesting` is an upgradeable contract, the owner can upgrade the contract without the community's commitment. If an attacker compromises the account, he can change the implementation of the contract and drain tokens from the contract.

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

`[Iskra]` : It's known issue for us.

- Since this contract is used for employees or contract partners, not for ordinary people, it was judged that being able to respond to various accident situations is more important than decentralization.
- The owner's authority is planned to be managed with a multi-signal wallet.

INF-03 | BATCHMINTING DOES NOT PREVENT OVERFLOW

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/token/ERC721/ItemNFT.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 76~77	● Acknowledged

Description

The function `ERC721._mint()` updates the receiver balance as follows:

```
        unchecked {
            // Will not overflow unless all 2**256 token ids are minted to the same
owner.
            // Given that tokens are minted one by one, it is impossible in practice
that
            // this ever happens. Might change if we allow batch minting.
            // The ERC fails to describe this case.
            _balances[to] += 1;
        }
```

In theory, the function `safeMintBatch()` could cause an overflow.

Recommendation

We recommend adding checks to prevent balance overflow.

Alleviation

`[Iskra]` : In batch minting, the internal logic is not that different, so it is impossible to mint 2**256 token ids to the same owner as well due to the gas system.

VET-04 | UNPROTECTED INITIALIZER

Category	Severity	Location	Status
Coding Style	● Minor	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 47	● 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 privileged operations that trick unsuspecting users into believing that she is the owner of the upgradeable contract.

```
10  contract Vesting is OwnableUpgradeable {
```

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

```
47      function initialize() public initializer {
```

- `initialize` is an unprotected initializer function.

Recommendation

We advise calling `_disableInitializers` in the constructor or giving 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

`[CertiK]` : The team heeded the advice and resolved the finding, commit: 35d8e5d0b33148111b9d25a0e1cfd96f80bcf2e1.

VET-05 | UNCHECKED ERC-20 `transfer()` / `transferFrom()` CALL

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 93~97, 146, 169	● Resolved

Description

The return value of the transfer()/transferFrom() call is not checked.

```
93          token.transferFrom(
94              _distributor,
95              address(this),
96              initialVestingAmount * 10**18
97          );
```

```
146             token.transfer(_reclaimer, _amount);
```

```
169         token.transfer(beneficiary, _amount * 10**18);
```

Recommendation

Since some ERC-20 tokens return no values and others return a `bool` value, they should be handled with care. We advise using the OpenZeppelin's `SafeERC20.sol` implementation to interact with the `transfer()` and `transferFrom()` functions of external ERC-20 tokens. The OpenZeppelin implementation checks for the existence of a return value and reverts if `false` is returned, making it compatible with all ERC-20 token implementations.

Alleviation

`[CertiK]` : The team heeded the advice and resolved the finding, commit: 61a6c049d099afc17e95005c5cb9f5b1251fec2b.

VET-06 | MISSING ZERO ADDRESS VALIDATION

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 187	● Resolved

Description

Addresses should be checked before assignment or external call to make sure they are not zero addresses.

```
187          beneficiary = _newBeneficiary;
```

- `_newBeneficiary` is not zero-checked before being used.

Recommendation

We recommend adding a zero-check for the passed-in address value to prevent unexpected errors.

Alleviation

`[CertiK]` : The team heeded the advice and resolved the finding, commit: 61a6c049d099afc17e95005c5cb9f5b1251fec2b.

VET-07 | CHECK EFFECT INTERACTION PATTERN VIOLATED

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 93~97, 98, 100~108, 146, 148, 150, 169, 170, 172	● Partially Resolved

Description

A reentrancy attack can occur when the contract creates a function that makes an external call to another untrusted contract before resolving any effects. If the attacker can control the untrusted contract, they can make a recursive call back to the original function, repeating interactions that would have otherwise not run after the external call resolved the effects.

This finding is considered minor because the reentrancy only causes out-of-order events.

Recommendation

We recommend using the Checks-Effects-Interactions Pattern to avoid the risk of calling unknown contracts.
In the functions `prepare()`, `revoke()`, and `claim()`; having the call for external transfer functions at the end would follow the pattern.

Alleviation

`[CertiK]`: External calls now take place after most of variables updates, however some are still modified after the call and events are still emitted after.
Commit: 61a6c049d099afc17e95005c5cb9f5b1251fec2b.

VET-10 | THIRD PARTY DEPENDENCY

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 34	● Acknowledged

Description

The contract is serving as the underlying entity to interact with one third-party protocol. The scope of the audit treats third-party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of third parties can possibly create severe impacts, such as increasing fees of third parties, migrating to new LP pools, etc.

```
34      IERC20 public token;
```

- The contract `Vesting` interacts with a third-party contract with `IERC20` interface via `token`.

Recommendation

We understand that business logic requires interaction with third parties. We encourage the team to constantly monitor the statuses of third parties to mitigate the side effects when unexpected activities are observed.

Alleviation

`[Iskra]` : We will use this contract only with the tokens we implemented.

VET-11 | INCOMPATIBILITY WITH DEFLATIONARY TOKENS

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 93~97, 146, 169	● Resolved

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 the `Vesting` contract, only 90 tokens actually arrive 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.

Recommendation

We recommend regulating the set of pool tokens supported and adding necessary mitigation mechanisms to keep track of accurate balances if there is a need to support deflationary tokens.

Alleviation

`[CertiK]` : The team heeded the advice and resolved the finding, commit: 61a6c049d099afc17e95005c5cb9f5b1251fec2b.

VET-12 | MISSING INPUT VALIDATION ON `_reclaimer`

Category	Severity	Location	Status
Control Flow, Logical Issue	● Minor	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d37 4edaf5f2e665): 146	● Resolved

Description

In the contract `Vesting.sol`, the function `revoke()` should have a check preventing `_reclaimer == address(this)`. If the `_reclaimer` parameter is mistakenly set as the address of the contract, all tokens will stay in `Vesting`, and since after the transfer the `VestingStatus` is set as `REVOKED` it will be impossible to retrieve the tokens.

Recommendation

We recommend adding a check ensuring the balance of the contract is equal to zero in the function `revoke()`.

Alleviation

`[CertiK]`: The team heeded the advice and resolved the finding, commit: 61a6c049d099afc17e95005c5cb9f5b1251fec2b.

VET-02 | INACCURATE TRANSFER AMOUNT

Category	Severity	Location	Status
Mathematical Operations, Logical Issue	● Informational	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 96~97, 169	● Acknowledged

Description

In `Vesting.sol` , the functions `prepare()` and `claim()` transfer specific amounts of tokens. However, in the linked locations the amount is multiplied by 1e18 in the transfer functions.

The functions `transfer()` and `transferFrom()` from an ERC20 are already supposed to work without multiplying the amount by the decimals.

Recommendation

We recommend removing the 10**18 factor from the linked locations.

Alleviation

`[Iskra]` : `Prepare()` corresponds to deposit, and `claim()` corresponds to withdraw. These two functions must be moved in units of 10**18, and there is no problem because the input and output are the same unit.

`[CertiK]` : There is no inconsistency in deposit, removal, and revoking.
However, multiplying by 1e18 can cause unexpected mistakes, for example:

1. the owner wants to deposit 10 tokens, she approves the `Vesting` contract for this specific amount
2. the contract tries to transfer 10 * 10**18 tokens and it fails

OPTIMIZATIONS | ISKRA - AUDIT FOR TOKEN (PART 1)

ID	Title	Category	Severity	Status
GTE-02	`Ownable2Step` Is Never Used	Volatile Code, Gas Optimization	Optimization	● Resolved
TOK-01	Inefficient Memory Parameter	Gas Optimization	Optimization	● Resolved
VET-08	Unnecessary Check	Gas Optimization	Optimization	● Resolved
VET-09	Checked Arithmetic Is Unnecessary	Gas Optimization	Optimization	● Resolved

GTE-02 | `Ownable2Step` IS NEVER USED

Category	Severity	Location	Status
Volatile Code, Gas Optimization	● Optimization	contracts/token/ERC20/GameToken.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 7~8, 22	● Resolved

Description

The contract `GameToken` is importing and inheriting the `Ownable2Step` contract, however, the `onlyOwner` modifier is never used in the contract.

Recommendation

We recommend removing the import and inheritance of `Ownable2Step` since the ownership feature is not used in this contract.

Alleviation

`[CertiK]` : The team heeded the advice and resolved the finding, commit: 8e2b3b6969c7422bb822a81ebd7b3d3f7e656b52.

TOK-01 | INEFFICIENT MEMORY PARAMETER

Category	Severity	Location	Status
Gas Optimization	● Optimization	contracts/token/ERC1155/MultiToken.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 60, 64, 125, 132, 133, 134; contracts/token/ERC721/ItemNFT.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 115	● Resolved

Description

One or more parameters with `memory` data location are never modified in their functions and those functions are never called internally within the contract. Thus, their data location can be changed to `calldata` to avoid the gas consumption copying from calldata to memory.

```
14      function setURI(string memory newuri) public {
```

`setURI` has memory location parameters: `newuri` .

```
18      function mint(
```

`mint` has memory location parameters: `data` .

```
27      function mintBatch(
```

`mintBatch` has memory location parameters: `ids` , `values` , `data` .

```
44      function burnBatch(
```

`burnBatch` has memory location parameters: `ids` , `values` .

```
60      function setURI(uint256 tokenId, string memory tokenURI_) public onlyOwner {
```

`setURI` has memory location parameters: `tokenURI_` .

```
64      function setBaseURI(string memory baseURI) public onlyOwner {
```

`setBaseURI` has memory location parameters: `baseURI` .

```
function mint(
```

`mint` has memory location parameters: `data`.

```
function mintBatch(
```

`mintBatch` has memory location parameters: `ids`, `amounts`, `data`.

```
function setTokenURI(uint256 tokenId, string memory _tokenURI)
```

`setTokenURI` has memory location parameters: `_tokenURI`.

Recommendation

We recommend changing the parameter's data location to `calldata` to save gas.

- For Solidity versions prior to 0.6.9, since public functions are not allowed to have `calldata` parameters, the function visibility also needs to be changed to `external`.
- For Solidity versions prior to 0.5.0, since parameter data location is implicit, changing the function visibility to `external` will change the parameter's data location to `calldata` as well.

Alleviation

`[CertiK]`: The team heeded the advice and resolved the finding, commit: 45cdb2e31cba8cb62b6ee3ca7ee274d0b8f33f27.

VET-08 | UNNECESSARY CHECK

Category	Severity	Location	Status
Gas Optimization	● Optimization	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 73~74	● Resolved

Description

In the contract `Vesting.sol` , the function `prepare()` performs the following checks:

```
71          require(_duration > 0, "Vesting:  `_duration` is 0");
72          // otherwise, claimer can claim all amount after first unlock period
73          require(_amount > 0, "Vesting: `_amount` is 0");
```

```
79          require(
80              _amount >= _duration,
81              "Vesting: _amount must be greater than _duration"
82          );
```

Since `_duration > 0` is enforced by the first **require** statement and `_amount >= _duration` is enforced by the third one, the `_amount > 0` is implied and:

```
74          require(_amount > 0, "Vesting: `_amount` is 0");
```

is redundant.

Recommendation

We recommend removing the aforementioned **require** statement.

Alleviation

`[CertiK]` : The team heeded the advice and resolved the finding, commit: b916d7506e85693020619493dfd4fc87f1bf296b.

VET-09 | CHECKED ARITHMETIC IS UNNECESSARY

Category	Severity	Location	Status
Gas Optimization	● Optimization	contracts/vesting/Vesting.sol (9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665): 90	● Resolved

Description

The contract `Vesting.sol` is using a solidity version greater than 0.8.0; this version has built-in checks in the compiler preventing overflow/underflow of arithmetic operators.

In the function `prepare()`, the varaible `_totalLocked` is computed as follow:

```
88          initialVestingAmount = _amount;
89          initialUnlockedAmount = _initialUnlocked;
90          uint256 _totalLocked = initialVestingAmount - initialUnlockedAmount;
```

meaning that `_totalLocked = _amount - _initialUnlocked`, hence any underflow is prevented by the following check:

```
74          require(
75              _amount >= _initialUnlocked,
76              "Vesting: `_initialUnlocked` is greater than `_amount`"
77          );
```

Recommendation

We recommend using unchecked arithmetic to optimize gas consumption.

Alleviation

`[CertiK]`: The team heeded the advice and resolved the finding, commit: b916d7506e85693020619493dfd4fc87f1bf296b.

FORMAL VERIFICATION | ISKRA - AUDIT FOR TOKEN (PART 1)

Formal guarantees about the behavior of smart contracts can be obtained by reasoning about properties relating to the entire contract (e.g. contract invariants) or to specific functions of the contract. Once such properties are proven to be valid, they guarantee that the contract behaves as specified by the property. As part of this audit, we applied automated formal verification (symbolic model checking) to prove that well-known functions in the smart contracts adhere to their expected behavior.

Considered Functions And Scope

In the following, we provide a description of the properties that have been used in this audit. They are grouped according to the type of contract they apply to.

Verification of ERC-20 Compliance

We verified properties of the public interface of those token contracts that implement the ERC-20 interface. This covers

- Functions `transfer` and `transferFrom` that are widely used for token transfers,
- functions `approve` and `allowance` that enable the owner of an account to delegate a certain subset of her tokens to another account (i.e. to grant an allowance), and
- the functions `balanceOf` and `totalSupply` , which are verified to correctly reflect the internal state of the contract.

The properties that were considered within the scope of this audit are as follows:

Property Name	Title
erc20-transfer-revert-zero	`transfer` Prevents Transfers to the Zero Address
erc20-transfer-correct-amount	`transfer` Transfers the Correct Amount in Non-self Transfers
erc20-transfer-succeed-self	`transfer` Succeeds on Admissible Self Transfers
erc20-transfer-succeed-normal	`transfer` Succeeds on Admissible Non-self Transfers
erc20-transfer-correct-amount-self	`transfer` Transfers the Correct Amount in Self Transfers
erc20-transfer-change-state	`transfer` Has No Unexpected State Changes
erc20-transfer-exceed-balance	`transfer` Fails if Requested Amount Exceeds Available Balance
erc20-transfer-false	If `transfer` Returns `false` , the Contract State Is Not Changed
erc20-transfer-never-return-false	`transfer` Never Returns `false`
erc20-transfer-recipient-overflow	`transfer` Prevents Overflows in the Recipient's Balance

Property Name	Title
erc20-transferfrom-revert-from-zero	`transferFrom` Fails for Transfers From the Zero Address
erc20-transferfrom-revert-to-zero	`transferFrom` Fails for Transfers To the Zero Address
erc20-transferfrom-correct-amount	`transferFrom` Transfers the Correct Amount in Non-self Transfers
erc20-transferfrom-correct-amount-self	`transferFrom` Performs Self Transfers Correctly
erc20-transferfrom-succeed-normal	`transferFrom` Succeeds on Admissible Non-self Transfers
erc20-transferfrom-succeed-self	`transferFrom` Succeeds on Admissible Self Transfers
erc20-transferfrom-correct-allowance	`transferFrom` Updated the Allowance Correctly
erc20-transferfrom-change-state	`transferFrom` Has No Unexpected State Changes
erc20-transferfrom-fail-exceed-balance	`transferFrom` Fails if the Requested Amount Exceeds the Available Balance
erc20-transferfrom-fail-exceed-allowance	`transferFrom` Fails if the Requested Amount Exceeds the Available Allowance
erc20-transferfrom-false	If `transferFrom` Returns `false` , the Contract's State Is Unchanged
erc20-transferfrom-never-return-false	`transferFrom` Never Returns `false`
erc20-totalsupply-succeed-always	`totalSupply` Always Succeeds
erc20-totalsupply-correct-value	`totalSupply` Returns the Value of the Corresponding State Variable
erc20-totalsupply-change-state	`totalSupply` Does Not Change the Contract's State
erc20-balanceof-succeed-always	`balanceOf` Always Succeeds
erc20-transferfrom-fail-recipient-overflow	`transferFrom` Prevents Overflows in the Recipient's Balance
erc20-balanceof-correct-value	`balanceOf` Returns the Correct Value
erc20-balanceof-change-state	`balanceOf` Does Not Change the Contract's State
erc20-allowance-succeed-always	`allowance` Always Succeeds
erc20-allowance-correct-value	`allowance` Returns Correct Value
erc20-allowance-change-state	`allowance` Does Not Change the Contract's State

Property Name	Title
erc20-approve-revert-zero	`approve` Prevents Approvals For the Zero Address
erc20-approve-succeed-normal	`approve` Succeeds for Admissible Inputs
erc20-approve-correct-amount	`approve` Updates the Approval Mapping Correctly
erc20-approve-change-state	`approve` Has No Unexpected State Changes
erc20-approve-false	If `approve` Returns `false` , the Contract's State Is Unchanged
erc20-approve-never-return-false	`approve` Never Returns `false`

Verification of ERC-721 Compliance

We verified the properties of the public interface of those token contracts that implement the ERC-721 interface without pause.

The properties that were considered within the scope of this audit are as follows:

Property Name	Title
erc721-balanceof-succeed-normal	`balanceOf` Succeeds on Admissible Inputs
erc721-supportsinterface-correct-erc721	`supportsInterface` Signals Support for `ERC721`
erc721-balanceof-correct-count	`balanceOf` Returns the Correct Value
erc721-balanceof-revert	`balanceOf` Fails on the Zero Address
erc721-balanceof-no-change-state	`balanceOf` Does Not Change the Contract's State
erc721-ownerof-succeed-normal	`ownerOf` Succeeds For Valid Tokens
erc721-ownerof-correct-owner	`ownerOf` Returns the Correct Owner
erc721-ownerof-revert	`ownerOf` Fails On Invalid Tokens
erc721-ownerof-no-change-state	`ownerOf` Does Not Change the Contract's State
erc721-getapproved-succeed-normal	`getApproved` Succeeds For Valid Tokens
erc721-getapproved-correct-value	`getApproved` Returns Correct Approved Address
erc721-getapproved-revert-zero	`getApproved` Fails on Invalid Tokens
erc721-isapprovedforall-succeed-normal	`isApprovedForAll` Always Succeeds

Property Name	Title
erc721-isapprovedforall-correct	`isApprovedForAll` Returns Correct Approvals
erc721-getapproved-change-state	`getApproved` Does Not Change the Contract's State
erc721-isapprovedforall-change-state	`isApprovedForAll` Does Not Change the Contract's State
erc721-approve-set-correct	`approve` Sets Approval
erc721-approve-succeed-normal	`approve` Returns for Admissible Inputs
erc721-approve-revert-not-allowed	`approve` Prevents Unpermitted Approvals
erc721-approve-revert-invalid-token	`approve` Fails For Calls with Invalid Tokens
erc721-approve-change-state	`approve` Has No Unexpected State Changes
erc721-setapprovalforall-succeed-normal	`setApprovalForAll` Returns for Admissible Inputs
erc721-setapprovalforall-set-correct	`setApprovalForAll` Approves Operator
erc721-setapprovalforall-multiple	`setApprovalForAll` Can Set Multiple Operators
erc721-setapprovalforall-change-state	`setApprovalForAll` Has No Unexpected State Changes
erc721-transferfrom-succeed-normal	`transferFrom` Succeeds on Admissible Inputs
erc721-transferfrom-correct-one-token-self	`transferFrom` Performs Self Transfers Correctly
erc721-transferfrom-correct-increase	`transferFrom` Transfers the Complete Token in Non-self Transfers
erc721-transferfrom-correct-approval	`transferFrom` Updates the Approval Correctly
erc721-transferfrom-correct-owner-from	`transferFrom` Removes Token Ownership of From
erc721-transferfrom-correct-owner-to	`transferFrom` Transfers Ownership
erc721-transferfrom-correct-balance	`transferFrom` Sum of Balances is Constant
erc721-transferfrom-correct-state-balance	`transferFrom` Keeps Balances Constant Except for From and To
erc721-transferfrom-correct-state-owner	`transferFrom` Has Expected Ownership Changes
erc721-transferfrom-correct-state-approval	`transferFrom` Has Expected Approval Changes
erc721-transferfrom-revert-invalid	`transferFrom` Fails for Invalid Tokens

Property Name	Title
erc721-transferfrom-revert-from-zero	`transferFrom` Fails for Transfers From the Zero Address
erc721-transferfrom-revert-to-zero	`transferFrom` Fails for Transfers To the Zero Address
erc721-supportsinterface-metadata	`supportsInterface` Signals that ERC721Metadata is Implemented
erc721-supportsinterface-enumerable	`supportsInterface` Signals that ERC721Enumerable is Implemented
erc721-totalsupply-succeed-always	`totalSupply` Always Succeeds
erc721-totalsupply-change-state	`totalSupply` Does Not Change the Contract's State
erc721-tokenofownerbyindex-revert	`tokenOfOwnerByIndex` Correctly Fails on Token Owner Indices Greater as the Owner Balance
erc721-supportsinterface-succeed-always	`supportsInterface` Always Succeeds
erc721-supportsinterface-correct-erc165	`supportsInterface` Signals Support for ERC165
erc721-supportsinterface-correct-false	`supportsInterface` Returns `False` for Id 0xffffffff
erc721-supportsinterface-no-change-state	`supportsInterface` Does Not Change the Contract's State
erc721-transferfrom-revert-not-owned	`transferFrom` Fails if `From` Is Not Token Owner
erc721-transferfrom-revert-exceed-approval	`transferFrom` Fails for Token Transfers without Approval

Verification Results

In the remainder of this section, we list all contracts where model checking of at least one property was not successful. There are several reasons why this could happen:

- Model checking reports a counterexample that violates the property. Depending on the counterexample,this occurs if
  - The specification of the property is too generic and does not accurately capture the intended behavior of the smart contract. In that case, the counterexample does not indicate a problem in the underlying smart contract. We report such instances as being "inapplicable".
  - The property is applicable to the smart contract. In that case, the counterexample showcases a problem in the smart contract and a correspond finding is reported separately in the Findings section of this report. In the following tables, we report such instances as "invalid". The distinction between spurious and actual counterexamples is done manually by the auditors.
- The model checking result is inconclusive. Such a result does not indicate a problem in the underlying smart contract. An inconclusive result may occur if

- The model checking engine fails to construct a proof. This can happen if the logical deductions necessary are beyond the capabilities of the automated reasoning tool. It is a technical limitation of all proof engines and cannot be avoided in general.
- The model checking engine runs out of time or memory and did not produce a result. This can happen if automatic abstraction techniques are ineffective or of the state space is too big.

Detailed Results For Contract GameToken (contracts/token/ERC20/GameToken.sol) In Commit 9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665

Verification of ERC-20 Compliance

Detailed results for function `transfer`

Property Name	Final Result	Remarks
erc20-transfer-revert-zero	● True	
erc20-transfer-correct-amount	● True	
erc20-transfer-succeed-self	○ Inapplicable	Intended behavior
erc20-transfer-succeed-normal	○ Inapplicable	Intended behavior
erc20-transfer-correct-amount-self	● True	
erc20-transfer-change-state	● True	
erc20-transfer-exceed-balance	● True	
erc20-transfer-false	● True	
erc20-transfer-never-return-false	● True	
erc20-transfer-recipient-overflow	○ Inapplicable	Context not considered

Detailed results for function `transferFrom`

Property Name	Final Result	Remarks
erc20-transferfrom-revert-from-zero	● True	
erc20-transferfrom-revert-to-zero	● True	
erc20-transferfrom-correct-amount	● True	
erc20-transferfrom-correct-amount-self	● True	
erc20-transferfrom-succeed-normal	● Inapplicable	Intended behavior
erc20-transferfrom-succeed-self	● Inapplicable	Intended behavior
erc20-transferfrom-correct-allowance	● True	
erc20-transferfrom-change-state	● True	
erc20-transferfrom-fail-exceed-balance	● True	
erc20-transferfrom-fail-exceed-allowance	● True	
erc20-transferfrom-false	● True	
erc20-transferfrom-never-return-false	● True	
erc20-transferfrom-fail-recipient-overflow	● Inapplicable	Context not considered

Detailed results for function `totalSupply`

Property Name	Final Result	Remarks
erc20-totalsupply-succeed-always	● True	
erc20-totalsupply-correct-value	● True	
erc20-totalsupply-change-state	● True	

Detailed results for function `balanceOf`

Property Name	Final Result	Remarks
erc20-balanceof-succeed-always	● True	
erc20-balanceof-correct-value	● True	
erc20-balanceof-change-state	● True	

Detailed results for function `allowance`

Property Name	Final Result	Remarks
erc20-allowance-succeed-always	● True	
erc20-allowance-correct-value	● True	
erc20-allowance-change-state	● True	

Detailed results for function `approve`

Property Name	Final Result	Remarks
erc20-approve-revert-zero	● True	
erc20-approve-succeed-normal	● True	
erc20-approve-correct-amount	● True	
erc20-approve-change-state	● True	
erc20-approve-false	● True	
erc20-approve-never-return-false	● True	

Detailed Results For Contract UtilityToken (contracts/token/ERC20/UtilityToken.sol) In Commit 9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665

Verification of ERC-20 Compliance

Detailed results for function `transfer`

Property Name	Final Result	Remarks
erc20-transfer-revert-zero	● True	
erc20-transfer-succeed-normal	● Inapplicable	Intended behavior
erc20-transfer-succeed-self	● Inapplicable	Intended behavior
erc20-transfer-correct-amount-self	● True	
erc20-transfer-correct-amount	● True	
erc20-transfer-change-state	● True	
erc20-transfer-false	● True	
erc20-transfer-exceed-balance	● True	
erc20-transfer-never-return-false	● True	
erc20-transfer-recipient-overflow	● Inapplicable	Context not considered

Detailed results for function `transferFrom`

Property Name	Final Result	Remarks
erc20-transferfrom-revert-from-zero	● True	
erc20-transferfrom-revert-to-zero	● True	
erc20-transferfrom-correct-amount-self	● True	
erc20-transferfrom-correct-amount	● True	
erc20-transferfrom-succeed-normal	● Inapplicable	Intended behavior
erc20-transferfrom-succeed-self	● Inapplicable	Intended behavior
erc20-transferfrom-change-state	● True	
erc20-transferfrom-correct-allowance	● True	
erc20-transferfrom-fail-exceed-balance	● True	
erc20-transferfrom-fail-exceed-allowance	● True	
erc20-transferfrom-false	● True	
erc20-transferfrom-never-return-false	● True	
erc20-transferfrom-fail-recipient-overflow	● Inapplicable	Context not considered

Detailed results for function `totalSupply`

Property Name	Final Result	Remarks
erc20-totalsupply-succeed-always	● True	
erc20-totalsupply-correct-value	● True	
erc20-totalsupply-change-state	● True	

Detailed results for function `balanceOf`

Property Name	Final Result	Remarks
erc20-balanceof-succeed-always	● True	
erc20-balanceof-correct-value	● True	
erc20-balanceof-change-state	● True	

Detailed results for function `allowance`

Property Name	Final Result	Remarks
erc20-allowance-succeed-always	● True	
erc20-allowance-correct-value	● True	
erc20-allowance-change-state	● True	

Detailed results for function `approve`

Property Name	Final Result	Remarks
erc20-approve-revert-zero	● True	
erc20-approve-succeed-normal	● True	
erc20-approve-correct-amount	● True	
erc20-approve-change-state	● True	
erc20-approve-false	● True	
erc20-approve-never-return-false	● True	

Detailed Results For Contract ItemNFT (contracts/token/ERC721/ItemNFT.sol) In Commit 9fbf5a5e53eb0cf74d08d28b4d374edaf5f2e665

Verification of ERC-721 Compliance

Detailed results for function `balanceOf`

Property Name	Final Result	Remarks
erc721-balanceof-succeed-normal	● True	
erc721-balanceof-correct-count	● True	
erc721-balanceof-revert	● True	
erc721-balanceof-no-change-state	● True	

Detailed results for function `supportsInterface`

Property Name	Final Result	Remarks
erc721-supportsinterface-correct-erc721	● True	
erc721-supportsinterface-metadata	● True	
erc721-supportsinterface-enumerable	● True	
erc721-supportsinterface-succeed-always	● True	
erc721-supportsinterface-correct-erc165	● True	
erc721-supportsinterface-correct-false	● True	
erc721-supportsinterface-no-change-state	● True	

Detailed results for function `ownerOf`

Property Name	Final Result	Remarks
erc721-ownerof-succeed-normal	● True	
erc721-ownerof-correct-owner	● True	
erc721-ownerof-revert	● True	
erc721-ownerof-no-change-state	● True	

Detailed results for function `getApproved`

Property Name	Final Result	Remarks
erc721-getapproved-succeed-normal	● True	
erc721-getapproved-correct-value	● True	
erc721-getapproved-revert-zero	● True	
erc721-getapproved-change-state	● True	

Detailed results for function `isApprovedForAll`

Property Name	Final Result	Remarks
erc721-isapprovedforall-succeed-normal	● True	
erc721-isapprovedforall-correct	● True	
erc721-isapprovedforall-change-state	● True	

Detailed results for function `approve`

Property Name	Final Result	Remarks
erc721-approve-set-correct	● True	
erc721-approve-succeed-normal	● True	
erc721-approve-revert-not-allowed	● True	
erc721-approve-revert-invalid-token	● True	
erc721-approve-change-state	● True	

Detailed results for function `setApprovalForAll`

Property Name	Final Result	Remarks
erc721-setapprovalforall-succeed-normal	● True	
erc721-setapprovalforall-set-correct	● True	
erc721-setapprovalforall-multiple	● True	
erc721-setapprovalforall-change-state	● True	

Detailed results for function `transferFrom`

Property Name	Final Result	Remarks
erc721-transferfrom-succeed-normal	● Inapplicable	Intended behavior
erc721-transferfrom-correct-one-token-self	● True	
erc721-transferfrom-correct-increase	● True	
erc721-transferfrom-correct-approval	● True	
erc721-transferfrom-correct-owner-from	● True	
erc721-transferfrom-correct-owner-to	● True	
erc721-transferfrom-correct-balance	● True	
erc721-transferfrom-correct-state-balance	● True	
erc721-transferfrom-correct-state-owner	● True	
erc721-transferfrom-correct-state-approval	● True	
erc721-transferfrom-revert-invalid	● True	
erc721-transferfrom-revert-from-zero	● True	
erc721-transferfrom-revert-to-zero	● True	
erc721-transferfrom-revert-not-owned	● True	
erc721-transferfrom-revert-exceed-approval	● True	

Detailed results for function `totalSupply`

Property Name	Final Result	Remarks
erc721-totalsupply-succeed-always	● True	
erc721-totalsupply-change-state	● True	

Detailed results for function `tokenOfOwnerByIndex`

Property Name	Final Result	Remarks
erc721-tokenofownerbyindex-revert	● True	

APPENDIX | ISKRA - AUDIT FOR TOKEN (PART 1)

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.
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.
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.

Details on Formal Verification

Some Solidity smart contracts from this project have been formally verified using symbolic model checking. Each such contract was compiled into a mathematical model which reflects all its possible behaviors with respect to the property. The model takes into account the semantics of the Solidity instructions found in the contract. All verification results that we report are based on that model.

Technical Description

The model also formalizes a simplified execution environment of the Ethereum blockchain and a verification harness that performs the initialization of the contract and all possible interactions with the contract. Initially, the contract state is initialized non-deterministically (i.e. by arbitrary values) and over-approximates the reachable state space of the contract throughout any actual deployment on chain. All valid results thus carry over to the contract's behavior in arbitrary states after it has been deployed.

Assumptions and Simplifications

The following assumptions and simplifications apply to our model:

- Gas consumption is not taken into account, i.e. we assume that executions do not terminate prematurely because they run out of gas.
- The contract's state variables are non-deterministically initialized before invocation of any function. That ignores contract invariants and may lead to false positives. It is, however, a safe over-approximation.
- The verification engine reasons about unbounded integers. Machine arithmetic is modeled using modular arithmetic based on the bit-width of the underlying numeric Solidity type. This ensures that over- and underflow characteristics are faithfully represented.
- Certain low-level calls and inline assembly are not supported and may lead to a contract not being formally verified.
- We model the semantics of the Solidity source code and not the semantics of the EVM bytecode in a compiled contract.

Formalism for Property Specification

All properties are expressed in linear temporal logic (LTL). For that matter, we treat each invocation of and each return from a public or an external function as a discrete time step. Our analysis reasons about the contract's state upon entering and upon leaving public or external functions.

Apart from the Boolean connectives and the modal operators "always" (written `[]`) and "eventually" (written `<>`), we use the following predicates as atomic propositions. They are evaluated on the contract's state whenever a discrete time step occurs:

- `started(f, [cond])` Indicates an invocation of contract function `f` within a state satisfying formula `cond`.
- `willSucceed(f, [cond])` Indicates an invocation of contract function `f` within a state satisfying formula `cond` and considers only those executions that do not revert.
- `finished(f, [cond])` Indicates that execution returns from contract function `f` in a state satisfying formula `cond`. Here, formula `cond` may refer to the contract's state variables and to the value they had upon entering the function (using the `old` function).
- `reverted(f, [cond])` Indicates that execution of contract function `f` was interrupted by an exception in a contract state satisfying formula `cond`.

The verification performed in this audit operates on a harness that non-deterministically invokes a function of the contract's public or external interface. All formulas are analyzed w.r.t. the trace that corresponds to this function invocation.

Description of the Analyzed ERC-20 Properties

The specifications are designed such that they capture the desired and admissible behaviors of the ERC-20 functions `transfer` , `transferFrom` , `approve` , `allowance` , `balanceOf` , and `totalSupply` . In the following, we list those property specifications.

Properties related to function `transfer`

erc20-transfer-revert-zero

`transfer` Prevents Transfers to the Zero Address. Any call of the form `transfer(recipient, amount)` must fail if the recipient address is the zero address. Specification:

```
[](started(contract.transfer(to, value), to == address(0)) ==>
  <>(reverted(contract.transfer) || finished(contract.transfer(to, value), return
    == false)))
```

erc20-transfer-succeed-normal

`transfer` Succeeds on Admissible Non-self Transfers. All invocations of the form `transfer(recipient, amount)` must succeed and return `true` if

- the `recipient` address is not the zero address,
- `amount` does not exceed the balance of address `msg.sender` ,
- transferring `amount` to the `recipient` address does not lead to an overflow of the recipient's balance, and
- the supplied gas suffices to complete the call. Specification:

```
[](started(contract.transfer(to, value), to != address(0) && to != msg.sender &&
    value >= 0 && value <= _balances[msg.sender] && _balances[to] + value <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[to] >= 0 && _balances[msg.sender] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transfer(to, value), return == true)))
```

erc20-transfer-succeed-self

`transfer` Succeeds on Admissible Self Transfers. All self-transfers, i.e. invocations of the form `transfer(recipient, amount)` where the `recipient` address equals the address in `msg.sender` must succeed and return `true` if

- the value in `amount` does not exceed the balance of `msg.sender` and
- the supplied gas suffices to complete the call. Specification:

```
[](started(contract.transfer(to, value), to != address(0) && to == msg.sender &&
    value >= 0 && value <= _balances[msg.sender] && _balances[msg.sender] >= 0 &&
    _balances[msg.sender] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transfer(to, value), return == true)))
```

erc20-transfer-correct-amount

`transfer` Transfers the Correct Amount in Non-self Transfers. All non-reverting invocations of `transfer(recipient, amount)` that return `true` must subtract the value in `amount` from the balance of `msg.sender` and add the same value to the balance of the `recipient` address. Specification:

```
[](willSucceed(contract.transfer(to, value), to != msg.sender && _balances[to] >= 0
    && value >= 0 && _balances[to] + value <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[msg.sender] >= 0 && _balances[msg.sender] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transfer(to, value), return == true ==>
      _balances[msg.sender] == old(_balances[msg.sender]) - value && _balances[to]
      == old(_balances[to]) + value)))
```

erc20-transfer-correct-amount-self

`transfer` Transfers the Correct Amount in Self Transfers. All non-reverting invocations of `transfer(recipient, amount)` that return `true` and where the `recipient` address equals `msg.sender` (i.e. self-transfers) must not change the balance of address `msg.sender`. Specification:

```
[](willSucceed(contract.transfer(to, value), to == msg.sender && _balances[to] >= 0
    && _balances[to] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transfer(to, value), return == true ==> _balances[to] ==
      old(_balances[to]))))
```

erc20-transfer-change-state

`transfer` Has No Unexpected State Changes. All non-reverting invocations of `transfer(recipient, amount)` that return `true` must only modify the balance entries of the `msg.sender` and the `recipient` addresses. Specification:

```
[](willSucceed(contract.transfer(to, value), p1 != msg.sender && p1 != to) ==>
  <>(finished(contract.transfer(to, value), return == true ==> (_totalSupply ==
        old(_totalSupply) && _allowances == old(_allowances) && _balances[p1] ==
        old(_balances[p1]) && other_state_variables ==
        old(other_state_variables)))))
```

erc20-transfer-exceed-balance

`transfer` Fails if Requested Amount Exceeds Available Balance. Any transfer of an amount of tokens that exceeds the balance of `msg.sender` must fail. Specification:

```
[](started(contract.transfer(to, value), value > _balances[msg.sender] &&
    _balances[msg.sender] >= 0 && value <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(reverted(contract.transfer) || finished(contract.transfer(to, value), return
      == false)))
```

erc20-transfer-recipient-overflow

`transfer` Prevents Overflows in the Recipient's Balance. Any invocation of `transfer(recipient, amount)` must fail if it causes the balance of the `recipient` address to overflow. Specification:

```
[](started(contract.transfer(to, value), to != msg.sender && _balances[to] + value
    >= 0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[to] >= 0 && _balances[to] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[msg.sender] <
    0x10000000000000000000000000000000000000000000000000000000000000000 && value >
    0 && value <= _balances[msg.sender]) ==> <>(reverted(contract.transfer) ||
    finished(contract.transfer(to, value), return == false) ||
    finished(contract.transfer(to, value), _balances[to] > old(_balances[to]) +
      value -
      0x10000000000000000000000000000000000000000000000000000000000000000)))
```

erc20-transfer-false

If `transfer` Returns `false`, the Contract State Is Not Changed. If the `transfer` function in contract `contract` fails by returning `false`, it must undo all state changes it incurred before returning to the caller. Specification:

```
[](willSucceed(contract.transfer(to, value)) ==> <>(finished(contract.transfer(to,
        value), return == false ==> (_balances == old(_balances) && _totalSupply ==
        old(_totalSupply) && _allowances == old(_allowances) &&
        other_state_variables == old(other_state_variables)))))
```

erc20-transfer-never-return-false

`transfer` Never Returns `false`. The transfer function must never return `false` to signal a failure. Specification:

```
[](!(finished(contract.transfer, return == false)))
```

Properties related to function `transferFrom`

erc20-transferfrom-revert-from-zero

`transferFrom` Fails for Transfers From the Zero Address. All calls of the form `transferFrom(from, dest, amount)` where the `from` address is zero, must fail. Specification:

```
[](started(contract.transferFrom(from, to, value), from == address(0)) ==>
  <>(reverted(contract.transferFrom) || finished(contract.transferFrom, return ==
      false)))
```

erc20-transferfrom-revert-to-zero

`transferFrom` Fails for Transfers To the Zero Address. All calls of the form `transferFrom(from, dest, amount)` where the `dest` address is zero, must fail. Specification:

```
[](started(contract.transferFrom(from, to, value), to == address(0)) ==>
  <>(reverted(contract.transferFrom) || finished(contract.transferFrom, return ==
      false)))
```

erc20-transferfrom-succeed-normal

`transferFrom` Succeeds on Admissible Non-self Transfers. All invocations of `transferFrom(from, dest, amount)` must succeed and return `true` if

- the value of `amount` does not exceed the balance of address `from` ,
- the value of `amount` does not exceed the allowance of `msg.sender` for address `from` ,
- transferring a value of `amount` to the address in `dest` does not lead to an overflow of the recipient's balance, and
- the supplied gas suffices to complete the call. Specification:

```
[](started(contract.transferFrom(from, to, value), from != address(0) && to !=
    address(0) && from != to && value <= _balances[from] && value <=
    _allowances[from][msg.sender] && _balances[to] + value <
    0x10000000000000000000000000000000000000000000000000000000000000000 && value >=
    0 && _balances[to] >= 0 && _balances[from] >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _allowances[from][msg.sender] >= 0 && _allowances[from][msg.sender] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transferFrom(from, to, value), return == true)))
```

erc20-transferfrom-succeed-self

`transferFrom` Succeeds on Admissible Self Transfers. All invocations of `transferFrom(from, dest, amount)` where the `dest` address equals the `from` address (i.e. self-transfers) must succeed and return `true` if:

- The value of `amount` does not exceed the balance of address `from` ,
- the value of `amount` does not exceed the allowance of `msg.sender` for address `from` , and
- the supplied gas suffices to complete the call. Specification:

```
[](started(contract.transferFrom(from, to, value), from != address(0) && from == to
    && value <= _balances[from] && value <= _allowances[from][msg.sender] && value
    >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _allowances[from][msg.sender] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transferFrom(from, to, value), return == true)))
```

erc20-transferfrom-correct-amount

`transferFrom` Transfers the Correct Amount in Non-self Transfers. All invocations of `transferFrom(from, dest, amount)` that succeed and that return `true` subtract the value in `amount` from the balance of address `from` and add the same value to the balance of address `dest` . Specification:

```
[](willSucceed(contract.transferFrom(from, to, value), from != to && value >= 0 &&
    _balances[from] >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[to] >= 0 && _balances[to] + value <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transferFrom(from, to, value), return == true ==>
      _balances[from] == old(_balances[from]) - value && _balances[to] ==
      old(_balances[to] + value))))
```

erc20-transferfrom-correct-amount-self

`transferFrom` Performs Self Transfers Correctly. All non-reverting invocations of `transferFrom(from, dest, amount)` that return `true` and where the address in `from` equals the address in `dest` (i.e. self-transfers) do not change the balance entry of the `from` address (which equals `dest`). Specification:

```
[](willSucceed(contract.transferFrom(from, to, value), from == to && value >= 0 &&
    value < 0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[from] >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transferFrom(from, to, value), return == true ==>
      _balances[from] == old(_balances[from]))))
```

erc20-transferfrom-correct-allowance

`transferFrom` Updated the Allowance Correctly. All non-reverting invocations of `transferFrom(from, dest, amount)` that return `true` must decrease the allowance for address `msg.sender` over address `from` by the value in `amount` . Specification:

```
[](willSucceed(contract.transferFrom(from, to, value), value >= 0 && value <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[from] >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[to] >= 0 && _balances[to] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _allowances[from][msg.sender] >= 0 && _allowances[from][msg.sender] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transferFrom(from, to, value), return == true ==>
      ((_allowances[from][msg.sender] == old(_allowances[from][msg.sender]) -
      value) || (_allowances[from][msg.sender] ==
      old(_allowances[from][msg.sender]) && (from == msg.sender ||
        old(_allowances[from][msg.sender]) ==
        0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF))))))
```

erc20-transferfrom-change-state

`transferFrom` Has No Unexpected State Changes. All non-reverting invocations of `transferFrom(from, dest, amount)` that return `true` may only modify the following state variables:

- The balance entry for the address in `dest` ,
- The balance entry for the address in `from` ,
- The allowance for the address in `msg.sender` for the address in `from` . Specification:

```
[](willSucceed(contract.transferFrom(from, to, amount), p1 != from && p1 != to &&
    (p2 != from || p3 != msg.sender)) ==> <>(finished(contract.transferFrom(from,
      to, amount), return == true ==> (_totalSupply == old(_totalSupply) &&
      _balances[p1] == old(_balances[p1]) && _allowances[p2][p3] ==
      old(_allowances[p2][p3]) && other_state_variables ==
      old(other_state_variables)))))
```

erc20-transferfrom-fail-exceed-balance

`transferFrom` Fails if the Requested Amount Exceeds the Available Balance. Any call of the form `transferFrom(from, dest, amount)` with a value for `amount` that exceeds the balance of address `from` must fail. Specification:

```
[](started(contract.transferFrom(from, to, value), value > _balances[from] &&
    _balances[from] >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(reverted(contract.transferFrom) || finished(contract.transferFrom, return ==
      false)))
```

erc20-transferfrom-fail-exceed-allowance

`transferFrom` Fails if the Requested Amount Exceeds the Available Allowance. Any call of the form `transferFrom(from,` `dest, amount)` with a value for `amount` that exceeds the allowance of address `msg.sender` must fail. Specification:

```
[](started(contract.transferFrom(from, to, value), msg.sender != from && value >
    _allowances[from][msg.sender] && _allowances[from][msg.sender] >= 0 && value <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(reverted(contract.transferFrom) || finished(contract.transferFrom(from, to,
      value), return == false)))
```

erc20-transferfrom-fail-recipient-overflow

`transferFrom` Prevents Overflows in the Recipient's Balance. Any call of `transferFrom(from, dest, amount)` with a value in `amount` whose transfer would cause an overflow of the balance of address `dest` must fail. Specification:

```
[](started(contract.transferFrom(from, to, value), from != to && _balances[to] +
    value >= 0x10000000000000000000000000000000000000000000000000000000000000000 &&
    value < 0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[to] >= 0 && _balances[to] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(reverted(contract.transferFrom) || finished(contract.transferFrom(from, to,
      value), return == false) || finished(contract.transferFrom(from, to,
      value), _balances[to] > old(_balances[to]) + value -
     0x10000000000000000000000000000000000000000000000000000000000000000)))
```

erc20-transferfrom-false

If `transferFrom` Returns `false`, the Contract's State Is Unchanged. If `transferFrom` returns `false` to signal a failure, it must undo all incurred state changes before returning to the caller. Specification:

```
[](willSucceed(contract.transferFrom(from, to, value)) ==>
  <>(finished(contract.transferFrom(from, to, value), return == false ==>
    (_balances == old(_balances) && _totalSupply == old(_totalSupply) &&
    _allowances == old(_allowances) && other_state_variables ==
    old(other_state_variables)))))
```

erc20-transferfrom-never-return-false

`transferFrom` Never Returns `false`. The `transferFrom` function must never return `false`. Specification:

```
[](!(finished(contract.transferFrom, return == false)))
```

Properties related to function `totalSupply`

erc20-totalsupply-succeed-always

`totalSupply` Always Succeeds. The function `totalSupply` must always succeeds, assuming that its execution does not run out of gas. Specification:

```
[](started(contract.totalSupply) ==> <>(finished(contract.totalSupply)))
```

erc20-totalsupply-correct-value

`totalSupply` Returns the Value of the Corresponding State Variable. The `totalSupply` function must return the value that is held in the corresponding state variable of contract contract. Specification:

```
[](willSucceed(contract.totalSupply) ==> <>(finished(contract.totalSupply, return
      == _totalSupply)))
```

erc20-totalsupply-change-state

`totalSupply` Does Not Change the Contract's State. The `totalSupply` function in contract contract must not change any state variables. Specification:

```
[](willSucceed(contract.totalSupply) ==> <>(finished(contract.totalSupply,
      _totalSupply == old(_totalSupply) && _balances == old(_balances) &&
      _allowances == old(_allowances) && other_state_variables ==
      old(other_state_variables))))
```

Properties related to function `balanceOf`

erc20-balanceof-succeed-always

`balanceOf` Always Succeeds. Function `balanceOf` must always succeed if it does not run out of gas. Specification:

```
[](started(contract.balanceOf) ==> <>(finished(contract.balanceOf)))
```

erc20-balanceof-correct-value

`balanceOf` Returns the Correct Value. Invocations of `balanceOf(owner)` must return the value that is held in the contract's balance mapping for address `owner`. Specification:

```
[](willSucceed(contract.balanceOf) ==> <>(finished(contract.balanceOf(owner),
      return == _balances[owner])))
```

erc20-balanceof-change-state

`balanceOf` Does Not Change the Contract's State. Function `balanceOf` must not change any of the contract's state variables. Specification:

```
[](willSucceed(contract.balanceOf) ==> <>(finished(contract.balanceOf(owner),
      _totalSupply == old(_totalSupply) && _balances == old(_balances) &&
      _allowances == old(_allowances) && other_state_variables ==
      old(other_state_variables))))
```

Properties related to function `allowance`

erc20-allowance-succeed-always

`allowance` Always Succeeds. Function `allowance` must always succeed, assuming that its execution does not run out of gas. Specification:

```
[](started(contract.allowance) ==> <>(finished(contract.allowance)))
```

erc20-allowance-correct-value

`allowance` Returns Correct Value. Invocations of `allowance(owner, spender)` must return the allowance that address `spender` has over tokens held by address `owner` . Specification:

```
[](willSucceed(contract.allowance(owner, spender)) ==>
  <>(finished(contract.allowance(owner, spender), return ==
    _allowances[owner][spender])))
```

erc20-allowance-change-state

`allowance` Does Not Change the Contract's State. Function `allowance` must not change any of the contract's state variables. Specification:

```
[](willSucceed(contract.allowance(owner, spender)) ==>
  <>(finished(contract.allowance(owner, spender), _totalSupply == old(_totalSupply)
    && _balances == old(_balances) && _allowances == old(_allowances) &&
    other_state_variables == old(other_state_variables))))
```

Properties related to function `approve`

erc20-approve-revert-zero

`approve` Prevents Approvals For the Zero Address. All calls of the form `approve(spender, amount)` must fail if the address in `spender` is the zero address. Specification:

```
[](started(contract.approve(spender, value), spender == address(0)) ==>
  <>(reverted(contract.approve) || finished(contract.approve(spender, value),
    return == false)))
```

erc20-approve-succeed-normal

`approve` Succeeds for Admissible Inputs. All calls of the form `approve(spender, amount)` must succeed, if

- the address in `spender` is not the zero address and
- the execution does not run out of gas. Specification:

```
[](started(contract.approve(spender, value), spender != address(0)) ==>
  <>(finished(contract.approve(spender, value), return == true)))
```

erc20-approve-correct-amount

`approve` Updates the Approval Mapping Correctly. All non-reverting calls of the form `approve(spender, amount)` that return `true` must correctly update the allowance mapping according to the address `msg.sender` and the values of `spender` and `amount`. Specification:

```
[](willSucceed(contract.approve(spender, value), spender != address(0) && value >=
    0 && value <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.approve(spender, value), return == true ==>
      _allowances[msg.sender][spender] == value)))
```

erc20-approve-change-state

`approve` Has No Unexpected State Changes. All calls of the form `approve(spender, amount)` must only update the allowance mapping according to the address `msg.sender` and the values of `spender` and `amount` and incur no other state changes. Specification:

```
[](willSucceed(contract.approve(spender, value), spender != address(0) && (p1 !=
      msg.sender || p2 != spender)) ==> <>(finished(contract.approve(spender,
        value), return == true ==> _totalSupply == old(_totalSupply) && _balances
      == old(_balances) && _allowances[p1][p2] == old(_allowances[p1][p2]) &&
      other_state_variables == old(other_state_variables))))
```

erc20-approve-false

If `approve` Returns `false`, the Contract's State Is Unchanged. If function `approve` returns `false` to signal a failure, it must undo all state changes that it incurred before returning to the caller. Specification:

```
[](willSucceed(contract.approve(spender, value)) ==>
  <>(finished(contract.approve(spender, value), return == false ==> (_balances ==
      old(_balances) && _totalSupply == old(_totalSupply) && _allowances ==
      old(_allowances) && other_state_variables == old(other_state_variables)))))
```

erc20-approve-never-return-false

`approve` Never Returns `false`. The function `approve` must never returns `false`. Specification:

```
[](!(finished(contract.approve, return == false)))
```

Description of ERC-721 Properties

The specifications are designed such that they capture the desired and admissible behaviors of the ERC-721 functions `transferFrom` , `balanceOf` , `ownerOf` , `getApproved` , `isApprovedForAll` , `approve` , `setApprovalForAll` `supportsInterface` , `tokenURI` , `tokenByIndex` , `tokenByIndex` , `decimals` and `totalSupply` . In the following, we list those property specifications.

Properties related to function `transferFrom`

erc721-transferfrom-succeed-normal

`transferFrom` Succeeds on Admissible Inputs. All invocations of `transferFrom(from, to, tokenId)` must succeed if

- address `from` is the owner of token `tokenId` ,
- the sender is approved to transfer token `tokenId` ,
- transferring the token to the address `to` does not lead to an overflow of the recipient's balance, and
- the supplied gas suffices to complete the call. Specification:

```
[](started(contract.transferFrom(from, to, tokenId), from != address(0) && to !=
    address(0) && _owner[tokenId]==from && ((from == msg.sender) ||
      (_approved[tokenId] == msg.sender) || _approvedAll[from][msg.sender]) &&
  _balances[to] >= 0 && _balances[from] >= 1 && _balances[to] <
  0x10000000000000000000000000000000000000000000000000000000000000000 - 1 &&
  _balances[from] <
  0x10000000000000000000000000000000000000000000000000000000000000000) ==> <>
finished(contract.transferFrom(from, to, tokenId)))
```

erc721-transferfrom-correct-increase

`transferFrom` Transfers the Complete Token in Non-self Transfers. All invocations of `transferFrom(from, to, tokenId)` that succeed must subtract a token from the balance of address `from` and add the token to the balance of address `to` . Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), from != to &&
    _balances[from] > 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[to] <
    0x10000000000000000000000000000000000000000000000000000000000000000 - 1 &&
    _balances[to] >= 0) ==> <>(finished(contract.transferFrom(from, to, tokenId),
      _balances[from] == (old(_balances[from]) - 1) && _balances[to] ==
      (old(_balances[to]) + 1))))
```

erc721-transferfrom-correct-one-token-self

`transferFrom` Performs Self Transfers Correctly. All non-reverting invocations of `transferFrom(from, to, tokenId)` that return `true` and where the address `from` equals the address `to` (i.e. self-transfers) must not change the balance entry of the address `from` (which equals `to`). Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), from == to &&
    _owner[tokenId] == from && _balances[from] >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000) ==>
  <>(finished(contract.transferFrom(from, to, tokenId), _balances[from] ==
      old(_balances[from]))))
```

erc721-transferfrom-correct-approval

`transferFrom` Updates the Approval Correctly. All non-reverting invocations of `transferFrom(from, to, tokenId)` that return must remove any approval for token `tokenId`. Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), p1 != address(0)) ==>
  <>(finished(contract.transferFrom(from, to, tokenId), (_approved[tokenId] !=
        p1))))
```

erc721-transferfrom-correct-owner-from

`transferFrom` Removes Token Ownership of From. All non-reverting and non-self invocations of `transferFrom(from, to, tokenId)` that return, must remove the ownership of token `tokenId` from address `from`. Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), from != to && from !=
    address(0) && to != address(0) && (msg.sender==from ||
      _approved[tokenId]==msg.sender || _approvedAll[from][msg.sender])) ==>
  <>(finished(contract.transferFrom(from, to, tokenId), (_owner[tokenId] !=
        from))))
```

erc721-transferfrom-correct-owner-to

`transferFrom` Transfers Ownership. All non-reverting invocations of `transferFrom(from, to, tokenId)` must transfer the ownership of token `tokenId` to the address `to`. Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), from != address(0) && to
    != address(0) && _balances[from] >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[to] >= 0 && _balances[to] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    (msg.sender==from || _approved[tokenId]==msg.sender ||
    _approvedAll[from][msg.sender])) ==> <>(finished(contract.transferFrom(from,
      to, tokenId), (_owner[tokenId] == to))))
```

erc721-transferfrom-correct-balance

`transferFrom` Sum of Balances is Constant. All non-reverting invocations of `transferFrom(from, to, tokenId)` must keep the sum of token balances constant. Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), from!=address(0) &&
    _balances[from]>0 && to!=address(0) && _balances[from] <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[to] <
    0x10000000000000000000000000000000000000000000000000000000000000000 - 1 &&
    _balances[to] >= 0) ==> <>(finished(contract.transferFrom(from, to, tokenId),
      (old(_balances[from])-_balances[from]) ==
    (_balances[to]-old(_balances[to])))))
```

erc721-transferfrom-correct-state-balance

`transferFrom` Keeps Balances Constant Except for From and To. All non-reverting invocations of `transferFrom(from, to, tokenId)` must only modify the balance of the addresses `from` and `to`. Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), p1 != from && p1 != to )
  ==> <>(finished(contract.transferFrom(from, to, tokenId), _balances[p1] ==
      old(_balances[p1]))))
```

erc721-transferfrom-correct-state-owner

`transferFrom` Has Expected Ownership Changes. All non-reverting invocations of `transferFrom(from, to, tokenId)` must only modify the ownership of token `tokenId`. Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), t1 != tokenId) ==>
  <>(finished(contract.transferFrom(from, to, tokenId), _owner[t1] ==
      old(_owner[t1]) && _owner[t1] == old(_owner[t1]))))
```

erc721-transferfrom-correct-state-approval

`transferFrom` Has Expected Approval Changes. All non-reverting invocations of `transferFrom(from, to, tokenId)` must remove only approvals for token `tokenId` Specification:

```
[](willSucceed(contract.transferFrom(from, to, tokenId), t1 != tokenId) ==>
  <>(finished(contract.transferFrom(from, to, tokenId), _approved[t1] ==
      old(_approved[t1]))))
```

erc721-transferfrom-revert-invalid

`transferFrom` Fails for Invalid Tokens. All calls of the form `transferFrom(from, to, tokenId)` must fail for any invalid token. Specification:

```
[](started(contract.transferFrom(from, to, tokenId), _owner[tokenId] == address(0))
  ==> <>(reverted(contract.transferFrom)))
```

erc721-transferfrom-revert-from-zero

`transferFrom` Fails for Transfers From the Zero Address. All calls of the form `transferFrom(from, to, tokenId)` must fail if the `from` address is zero. Specification:

```
[](started(contract.transferFrom(from, to, tokenId), from == address(0)) ==>
  <>(reverted(contract.transferFrom(from, to, tokenId))))
```

erc721-transferfrom-revert-to-zero

`transferFrom` Fails for Transfers To the Zero Address. All calls of the form `transferFrom(from, to, tokenId)` must fail if the address `to` is the zero address. Specification:

```
[](started(contract.transferFrom(from, to, tokenId), to == address(0)) ==>
  <>(reverted(contract.transferFrom(from, to, tokenId))))
```

erc721-transferfrom-revert-not-owned

`transferFrom` Fails if `From` Is Not Token Owner. Any call of the form `transferFrom(from, to, tokenId)` must fail if address 'from' is not the owner of token `tokenId`. Specification:

```
[](started(contract.transferFrom(from, to, tokenId), _owner[tokenId]!= from) ==>
  <>(reverted(contract.transferFrom)))
```

erc721-transferfrom-revert-exceed-approval

`transferFrom` Fails for Token Transfers without Approval. Any call of the form `transferFrom(from, to, tokenId)` must fail if the sender is neither the token owner nor an operator of the token owner nor approved for token `tokenId`. Specification:

```
[](started(contract.transferFrom(from, to, tokenId), msg.sender!=from &&
    _approved[tokenId]!=msg.sender && !_approvedAll[from][msg.sender]) ==>
  <>(reverted(contract.transferFrom)))
```

Properties related to function `supportsInterface`

erc721-supportsinterface-correct-erc721

`supportsInterface` Signals Support for `ERC721`. Invocations of `supportsInterface(id)` must signal that the interface `ERC721` is implemented. Specification:

```
[](willSucceed(contract.supportsInterface(id), id==0x80ac58cd) ==> <>
  finished(contract.supportsInterface(id), return==true))
```

erc721-supportsinterface-metadata

`supportsInterface` Signals that ERC721Metadata is Implemented. A call of `supportsInterface(interfaceId)` with the interface id of ERC721Metadata must return true. Specification:

```
[](willSucceed(contract.supportsInterface(interfaceId), interfaceId==0x5b5e139f)
  ==> <> finished(contract.supportsInterface(interfaceId), return==true))
```

erc721-supportsinterface-enumerable

`supportsInterface` Signals that ERC721Enumerable is Implemented. Invocations of `supportsInterface(interfaceId)` must signal the support of the interface `ERC721Enumerable` since it is implemented. Specification:

```
[](willSucceed(contract.supportsInterface(interfaceId), interfaceId==0x780e9d63)
  ==> <> finished(contract.supportsInterface(interfaceId), return==true))
```

erc721-supportsinterface-succeed-always

`supportsInterface` Always Succeeds. Function `supportsInterface` must always succeed if it does not run out of gas. Specification:

```
[](started(contract.supportsInterface(id)) ==> <>
  finished(contract.supportsInterface(id)))
```

erc721-supportsinterface-correct-erc165

`supportsInterface` Signals Support for ERC165. Invocations of `supportsInterface(id)` must signal that the interface `ERC165` is implemented. Specification:

```
[](willSucceed(contract.supportsInterface(id), id==0x01ffc9a7) ==> <>
  finished(contract.supportsInterface(id), return==true))
```

erc721-supportsinterface-correct-false

`supportsInterface` Returns `False` for Id 0xffffffff. Invocations of `supportsInterface(id)` with `id` 0xffffffff must return `false` . Specification:

```
[](willSucceed(contract.supportsInterface(id), id==0xffffffff) ==> <>
  finished(contract.supportsInterface(id), return==false))
```

erc721-supportsinterface-no-change-state

`supportsInterface` Does Not Change the Contract's State. Function `supportsInterface` must not change any of the contract's state variables. Specification:

```
[](willSucceed(contract.supportsInterface(id)) ==>
  <>(finished(contract.supportsInterface(id), other_state_variables ==
    old(other_state_variables))))
```

Properties related to function `balanceOf`

erc721-balanceof-succeed-normal

`balanceOf` Succeeds on Admissible Inputs. All invocations of `balanceOf(owner)` must succeed if the address `owner` is not zero and it does not run out of gas. Specification:

```
[](started(contract.balanceOf(owner), owner!=address(0)) ==>
  <>(finished(contract.balanceOf)))
```

erc721-balanceof-correct-count

`balanceOf` Returns the Correct Value. Invocations of `balanceOf(owner)` must return the value that is held in the balance mapping for address `owner` . Specification:

```
[](willSucceed(contract.balanceOf) ==> <>(finished(contract.balanceOf(owner),
      return == _balances[owner])))
```

erc721-balanceof-revert

`balanceOf` Fails on the Zero Address. Invocations of `balanceOf(owner)` must fail if the address `owner` is the zero address. Specification:

```
[](started(contract.balanceOf(owner), owner==address(0)) ==>
  <>(reverted(contract.balanceOf(owner))))
```

erc721-balanceof-no-change-state

`balanceOf` Does Not Change the Contract's State. Function `balanceOf` must not change any of the contract's state variables. Specification:

```
[](willSucceed(contract.balanceOf) ==> <>(finished(contract.balanceOf, _balances ==
      old(_balances) && other_state_variables == old(other_state_variables))))
```

Properties related to function `ownerOf`

erc721-ownerof-succeed-normal

`ownerOf` Succeeds For Valid Tokens. Function `ownerOf(token)` must always succeed for valid tokens if it does not run out of gas. Specification:

```
[](started(contract.ownerOf(token), _owner[token]!=address(0)) ==>
  <>(finished(contract.ownerOf)))
```

erc721-ownerof-correct-owner

`ownerOf` Returns the Correct Owner. Invocations of `ownerOf(token)` must return the owner for a valid token `token` that is held in the contract's owner mapping. Specification:

```
[](willSucceed(contract.ownerOf(token), _owner[token]!=address(0)) ==>
  <>(finished(contract.ownerOf(token), return == _owner[token])))
```

erc721-ownerof-revert

`ownerOf` Fails On Invalid Tokens. Invocations of `ownerOf(token)` must fail for an invalid token. Specification:

```
[](started(contract.ownerOf(token), _owner[token]==address(0)) ==>
  <>(reverted(contract.ownerOf(token))))
```

erc721-ownerof-no-change-state

`ownerOf` Does Not Change the Contract's State. Function `ownerOf` must not change any of the contract's state variables. Specification:

```
[](willSucceed(contract.ownerOf) ==> <>(finished(contract.ownerOf, _owner ==
      old(_owner) && other_state_variables == old(other_state_variables))))
```

Properties related to function `getApproved`

erc721-getapproved-succeed-normal

`getApproved` Succeeds For Valid Tokens. Function `getApproved` must always succeed for valid tokens, assuming that its execution does not run out of gas. Specification:

```
[](started(contract.getApproved(token), _owner[token]!=address(0)) ==>
  <>(finished(contract.getApproved)))
```

erc721-getapproved-correct-value

`getApproved` Returns Correct Approved Address. Invocations of `getApproved(token)` must return the approved address of a valid `token`. Specification:

```
[](willSucceed(contract.getApproved(token)) ==>
  <>(finished(contract.getApproved(token), return == _approved[token] || return ==
    address(0))))
```

erc721-getapproved-revert-zero

`getApproved` Fails on Invalid Tokens. Invocations of `getApproved(token)` with an invalid token must fail. Specification:

```
[](started(contract.getApproved(token), _owner[token]==address(0)) ==>
  <>(reverted(contract.getApproved)))
```

erc721-getapproved-change-state

`getApproved` Does Not Change the Contract's State. Function `getApproved` must not change any of the contract's state variables. Specification:

```
[](willSucceed(contract.getApproved) ==> <>(finished(contract.getApproved,
      _approved == old(_approved) && other_state_variables ==
      old(other_state_variables))))
```

Properties related to function `isApprovedForAll`

erc721-isapprovedforall-succeed-normal

`isApprovedForAll` Always Succeeds. Function `isApprovedForAll` does always succeed, assuming that its execution does not run out of gas. Specification:

```
[](started(contract.isApprovedForAll(owner, operator)) ==>
  <>(finished(contract.isApprovedForAll)))
```

erc721-isapprovedforall-correct

`isApprovedForAll` Returns Correct Approvals. Invocations of `isApprovedForAll(owner, operator)` must return whether a non-zero address `operator` is approved for tokens of a non-zero address `owner` , or return false. Specification:

```
[](willSucceed(contract.isApprovedForAll(owner, operator), owner!=address(0) &&
    operator!=address(0)) ==> <>(finished(contract.isApprovedForAll(owner,
        operator), return == _approvedAll[owner][operator])))
```

erc721-isapprovedforall-change-state

`isApprovedForAll` Does Not Change the Contract's State. Function `isApprovedForAll` does not change any of the contract's state variables. Specification:

```
[](willSucceed(contract.isApprovedForAll) ==>
  <>(finished(contract.isApprovedForAll, _approvedAll == old(_approvedAll) &&
    other_state_variables == old(other_state_variables))))
```

Properties related to function `approve`

erc721-approve-succeed-normal

`approve` Returns for Admissible Inputs. All calls of the form `approve(to, tokenId)` must return if

- the sender is the owner or an authorized operator of the owner
- the token `tokenId` is valid and
- the execution does not run out of gas. Specification:

```
[](started(contract.approve(to, tokenId), (_owner[tokenId]!=address(0)) &&
    (_owner[tokenId]==msg.sender || _approvedAll[_owner[tokenId]][msg.sender]) &&
  (_owner[tokenId]!=to)) ==> <>(finished(contract.approve)))
```

erc721-approve-set-correct

`approve` Sets Approval. Any returning call of the form `approve(to, tokenId)` must approve the address `to` for token `tokenId`. Specification:

```
[](willSucceed(contract.approve(to, tokenId), (_owner[tokenId]!=address(0)) &&
    (_owner[tokenId]==msg.sender || _approvedAll[_owner[tokenId]][msg.sender])) ==>
<>(finished(contract.approve(to, tokenId), _approved[tokenId]==to)))
```

erc721-approve-revert-not-allowed

`approve` Prevents Unpermitted Approvals. All calls of the form `approve(to, tokenId)` must fail if the message sender is not permitted to access token `tokenId`. Specification:

```
[](started(contract.approve(to, tokenId), _owner[tokenId]!=msg.sender &&
    !_approvedAll[_owner[tokenId]][msg.sender]) ==> <>(reverted(contract.approve)))
```

erc721-approve-revert-invalid-token

`approve` Fails For Calls with Invalid Tokens. All calls of the form `approve(to, tokenId)` must fail for an invalid token. Specification:

```
[](started(contract.approve(to, tokenId), _owner[tokenId] == address(0)) ==>
  <>(reverted(contract.approve)))
```

erc721-approve-change-state

`approve` Has No Unexpected State Changes. All calls of the form `approve(to, tokenId)` must only update the allowance mapping according to a valid token `tokenId` and the address `to`, and incur no other state changes. Specification:

```
[](willSucceed(contract.approve(approved, tokenId), t1!=tokenId) ==>
  <>(finished(contract.approve(approved, tokenId),
    _approved[t1]==old(_approved[t1]) && other_state_variables ==
    old(other_state_variables))))
```

Properties related to function `setApprovalForAll`

erc721-setapprovalforall-succeed-normal

`setApprovalForAll` Returns for Admissible Inputs. Calls of the form `setApprovalForAll(operator, approved)` must return if

- the message sender is not the `operator`,
- `operator` is not the zero address and
- the execution does not run out of gas. Specification:

```
[](started(contract.setApprovalForAll(operator, approved), (msg.sender!=operator)
    && (operator!=address(0))) ==> <>(finished(contract.setApprovalForAll)))
```

erc721-setapprovalforall-set-correct

`setApprovalForAll` Approves Operator. All non-reverting calls of the form `setApprovalForAll(operator, approved)` must set the approval of a non-zero address `operator` according to the Boolean value `approved`. Specification:

```
[](willSucceed(contract.setApprovalForAll(operator, approved),
    operator!=address(0)) ==> <>(finished(contract.setApprovalForAll(operator,
        approved), _approvedAll[msg.sender][operator]==approved)))
```

erc721-setapprovalforall-multiple

`setApprovalForAll` Can Set Multiple Operators. Calls of the form `setApprovalForAll(operator, approved)` must be able to set multiple operators for the tokens of the message sender. Specification:

```
[](willSucceed(contract.setApprovalForAll(operator, approved), op1!=address(0) &&
    approved && _approvedAll[msg.sender][op1]   ) ==>
  <>(finished(contract.setApprovalForAll(operator, approved),
    _approvedAll[msg.sender][operator] && _approvedAll[msg.sender][op1])))
```

erc721-setapprovalforall-change-state

`setApprovalForAll` Has No Unexpected State Changes. All calls of the form `setApprovalForAll(operator, approved)` must only update the approval mapping according to the message sender, the address `operator` and the Boolean value `approved` but incur no other state changes. Specification:

```
[](started(contract.setApprovalForAll(op, approved), ow1!=msg.sender || op1!=op)
  ==> <>(finished(contract.setApprovalForAll(op, approved),
      _approvedAll[ow1][op1]==old(_approvedAll[ow1][op1]) &&
      _approvedAll[msg.sender][op]==approved && other_state_variables ==
      old(other_state_variables)) || reverted(contract.setApprovalForAll(op,
        approved))))
```

Properties related to function `totalSupply`

erc721-totalsupply-succeed-always

`totalSupply` Always Succeeds. The function `totalSupply` must always succeed, assuming that its execution does not run out of gas. Specification:

```
[](started(contract.totalSupply) ==> <>(finished(contract.totalSupply)))
```

erc721-totalsupply-change-state

`totalSupply` Does Not Change the Contract's State. The `totalSupply` function in contract contract must not change any state variables. Specification:

```
[](willSucceed(contract.totalSupply) ==> <>(finished(contract.totalSupply, _total
      == old(_total) && _balances == old(_balances) && other_state_variables ==
      old(other_state_variables))))
```

Properties related to function `tokenOfOwnerByIndex`

erc721-tokenofownerbyindex-revert

`tokenOfOwnerByIndex` Correctly Fails on Token Owner Indices Greater as the Owner Balance. All calls of the form `tokenOfOwnerByIndex(owner, index)` must fail for token owner index `index` that are greater than the owner's balance. Specification:

```
[](started(contract.tokenOfOwnerByIndex(owner, index), _balances[owner]<=index ||
    owner==address(0)) ==> <> reverted(contract.tokenOfOwnerByIndex))
```

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.