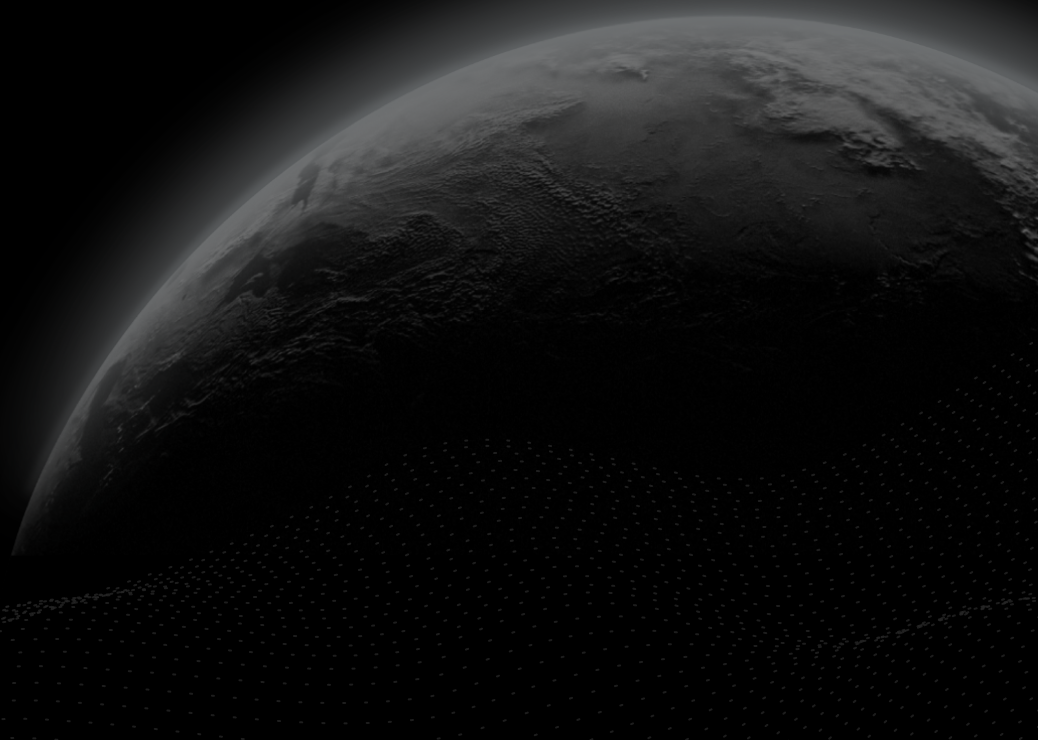
CERTIK

# Security Assessment

# GENEX

CertiK Assessed on Aug 1st, 2024



CertiK Assessed on Aug 1st, 2024

# GENEX

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

## Executive Summary

| TYPES | ECOSYSTEM | METHODS |
|---|---|---|
| ERC-20 | Binance Smart Chain (BSC) | Formal Verification, Manual Review, Static Analysis |

| LANGUAGE | TIMELINE | KEY COMPONENTS |
|---|---|---|
| Solidity | Delivered on 08/01/2024 | N/A |

| CODEBASE | COMMITS |
|---|---|
| mainnet | 0x98f06352dc8a40dd6d94d4cde3b384e2276c991a |
| View All in Codebase Page | View All in Codebase Page |

## Highlighted Centralization Risks

Initial owner token share is 100%

## Vulnerability Summary

| 4 | 0 | 0 | 0 | 4 | 0 |
|---|---|---|---|---|---|
| Total Findings | Resolved | Mitigated | Partially Resolved | Acknowledged | Declined |

| | | | |
|---|---|---|---|
| 0 Critical | | | Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks. |
| 1 Major | 1 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. |
| 1 Minor | 1 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. |
| 2 Informational | 2 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 | GENEX

# CODEBASE | GENEX

## Repository

mainnet

## Commit

0x98f06352dc8a40dd6d94d4cde3b384e2276c991a

# AUDIT SCOPE | GENEX

1 file audited ● 1 file with Acknowledged findings

| ID | Repo | File | SHA256 Checksum |
| --- | --- | --- | --- |
| ● GEN | mainnet | GENEX.sol | e960baf13dcccbcd519b2ad0eacbb34e20ebbd264ffa13b513d79ecf3309f8f8 |

# APPROACH & METHODS | GENEX

This report has been prepared for GENEX to discover issues and vulnerabilities in the source code of the GENEX 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 | GENEX

| 4 | 0 | 1 | 0 | 1 | 2 |
|---|---|---|---|---|---|
| Total Findings | Critical | Major | Medium | Minor | Informational |

This report has been prepared to discover issues and vulnerabilities for GENEX. Through this audit, we have uncovered 4 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 |
|---|---|---|---|---|
| **GEN-02** | **Initial Token Distribution** | **Centralization** | **Major** | **Acknowledged** |
| GLOBAL-01 | Potential Front-Run On Token Allowance Approval | Logical Issue | Minor | Acknowledged |
| GEN-03 | Unlocked Compiler Version | Language Version | Informational | Acknowledged |
| GEN-04 | Big Numbers Could Be Written In A Clearer Way | Coding Style | Informational | Acknowledged |

# GEN-02 | INITIAL TOKEN DISTRIBUTION

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| **Centralization** | **Major** | **GENEX.sol: 2184~2185** | **Acknowledged** |

## Description

All of the `GENEX` tokens are sent to the contract deployer or one or several externally-owned account (EOA) addresses. This is a centralization risk because the deployer or the owner(s) of the EOAs can distribute tokens without obtaining the consensus of the community. Any compromise to these addresses may allow a hacker to steal and sell tokens on the market, resulting in severe damage to the project.

## Recommendation

It is recommended that the team be transparent regarding the initial token distribution process. The token distribution plan should be published in a public location that the community can access. The team should make efforts to restrict access to the private keys of the deployer account or EOAs. A multi-signature (⅔, ⅗) wallet can be used to prevent a single point of failure due to a private key compromise. Additionally, the team can lock up a portion of tokens, release them with a vesting schedule for long-term success, and deanonymize the project team with a third-party KYC provider to create greater accountability.

## Alleviation

**[`CertiK`, 08/01/2024]**: The team acknowledged the issue and decided the keep the current codebase.

# GLOBAL-01 POTENTIAL FRONT-RUN ON TOKEN ALLOWANCE APPROVAL

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Logical Issue | Minor | | Acknowledged |

## Description

The OpenZeppelin v5 ERC20 contract strictly implements the EIP-20 specification only and it omits the `increaseAllowance()` and `decreaseAllowance()` methods which were meant to mitigate issues on the front-run of the `approve()` call.

In fact, the ERC20 interface exposes a vulnerability according to which `approve()` calls may be front-run allowing a malicious spender to:

1. spend the already granted allowance,
2. have the allowance restored by the `approve()` call,
3. leverage more allowance than though by the token owner.

The usage of `increaseAllowance()` and `decreaseAllowance()` do not solve the issue, but mitigates it by bounding the maximum amount of spendable tokens to the sum of the previous and newly granted allowance, avoiding any value replacement.

## Recommendation

We recommend including the `increaseAllowance()` and `decreaseAllowance()` methods in the GENEX token implementation to mitigate the described front-run condition.

The ERC-20 implementation in the OpenZeppelin v4 library can be taken as a reference. REF.

Alternatively, the `approve()` method may implement an additional constraint in which updates can only happen from a zero value, forcing a double transaction for each change.

In any case, the front-run risk is unchanged for the `decrease` scenario.

## Alleviation

**[`CertiK`, 08/01/2024]**: The team acknowledged the issue and decided the keep the current codebase.

# GEN-03 | UNLOCKED COMPILER VERSION

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Language Version | Informational | GENEX.sol: 6, 88, 116, 146, 311, 629, 670, 763, 940, 1358, 1404, 1500, 1589, 1726, 1851, 1882, 2043, 2093, 2177 | Acknowledged |

## Description

The contract in scope has an unlocked compiler version. An unlocked compiler version in the source code of the contract permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging, as compiler specific bugs may occur in the codebase that would be hard to identify over a span of multiple compiler versions rather than a specific one.

## Recommendation

We recommend the compiler version is instead locked at the lowest version possible that the contract can be compiled at. For example, for version `v0.8.2` the contract should contain the following line:

```
pragma solidity 0.8.2;
```

## Alleviation

**[`CertiK`, 08/01/2024]**: The team acknowledged the issue and decided the keep the current codebase.

# GEN-04 | BIG NUMBERS COULD BE WRITTEN IN A CLEARER WAY

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Coding Style | Informational | GENEX.sol: 2185 | Acknowledged |

## Description

The big number linked is hard to read, and it is hard to identify the order of magnitude of the numbers, decreasing the readability of the code. In particular, the following numbers could be rewritten more clearly:

```
612     uint256 totalSupply = 7000000000 * (10**decimals());
```

## Recommendation

We recommend rewriting the big number more clearly, for example, the previous numbers could be rewritten as `7_000_000_000` .

## Alleviation

**[`CertiK`, 08/01/2024]**: The team acknowledged the issue and decided the keep the current codebase.

# OPTIMIZATIONS | GENEX

| ID | Title | Category | Severity | Status |
| --- | --- | --- | --- | --- |
| GEN-01 | Inefficient `view` Functions | Coding Issue | Optimization | Acknowledged |

# GEN-01 | INEFFICIENT `view` FUNCTIONS

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Coding Issue | Optimization | GENEX.sol: 137~139 | Acknowledged |

## Description

One or more `view` functions always return the same constant value, leading to unnecessary gas costs.

```
137     function _contextSuffixLength() internal view virtual returns (uint256) {
```

- `Context._contextSuffixLength` always returns `0`.

## Recommendation

It is recommended to declare those functions as pure to save gas and improve contract efficiency.

## Alleviation

**[`CertiK`, 08/01/2024]**: The team acknowledged the issue and decided the keep the current codebase.

# FORMAL VERIFICATION | GENEX

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 formal verification to prove that important functions in the smart contracts adhere to their expected behaviors.

## 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-transferfrom-fail-exceed-allowance | `transferFrom` Fails if the Requested Amount Exceeds the Available Allowance |
| erc20-allowance-change-state | `allowance` Does Not Change the Contract's State |
| erc20-transfer-correct-amount | `transfer` Transfers the Correct Amount in Transfers |
| erc20-transferfrom-correct-amount | `transferFrom` Transfers the Correct Amount in Transfers |
| erc20-transferfrom-correct-allowance | `transferFrom` Updated the Allowance Correctly |
| erc20-transferfrom-fail-recipient-overflow | `transferFrom` Prevents Overflows in the Recipient's Balance |
| erc20-transfer-recipient-overflow | `transfer` Prevents Overflows in the Recipient's Balance |
| erc20-approve-false | If `approve` Returns `false`, the Contract's State Is Unchanged |
| erc20-allowance-succeed-always | `allowance` Always Succeeds |
| erc20-approve-revert-zero | `approve` Prevents Approvals For the Zero Address |

| Property Name | Title |
| --- | --- |
| erc20-approve-never-return-false | `approve` Never Returns `false` |
| erc20-approve-succeed-normal | `approve` Succeeds for Valid Inputs |
| erc20-totalsupply-correct-value | `totalSupply` Returns the Value of the Corresponding State Variable |
| erc20-balanceof-succeed-always | `balanceOf` Always Succeeds |
| erc20-balanceof-correct-value | `balanceOf` Returns the Correct Value |
| erc20-transfer-false | If `transfer` Returns `false`, the Contract State Is Not Changed |
| erc20-totalsupply-succeed-always | `totalSupply` Always Succeeds |
| erc20-allowance-correct-value | `allowance` Returns Correct Value |
| erc20-transferfrom-false | If `transferFrom` Returns `false`, the Contract's State Is Unchanged |
| erc20-transferfrom-never-return-false | `transferFrom` Never Returns `false` |
| erc20-approve-correct-amount | `approve` Updates the Approval Mapping Correctly |
| erc20-transfer-never-return-false | `transfer` Never Returns `false` |
| erc20-transfer-revert-zero | `transfer` Prevents Transfers to the Zero Address |
| erc20-transferfrom-revert-zero-argument | `transferFrom` Fails for Transfers with Zero Address Arguments |
| erc20-transfer-exceed-balance | `transfer` Fails if Requested Amount Exceeds Available Balance |
| erc20-balanceof-change-state | `balanceOf` Does Not Change the Contract's State |
| erc20-totalsupply-change-state | `totalSupply` Does Not Change the Contract's State |
| erc20-transferfrom-fail-exceed-balance | `transferFrom` Fails if the Requested Amount Exceeds the Available Balance |

## Verification Results

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

- False: The property is violated by the project.
- Inconclusive: The proof engine cannot prove or disprove the property due to timeouts or exceptions.
- Inapplicable: The property does not apply to the project.

## Detailed Results For Contract GENEX (GENEX.sol) In Commit 0x98f06352dc8a40dd6d94d4cde3b384e2276c991a

### Verification of ERC-20 Compliance

Detailed Results for Function `transferFrom`

| Property Name | Final Result | Remarks |
| --- | --- | --- |
| erc20-transferfrom-fail-exceed-allowance | True | |
| erc20-transferfrom-correct-amount | True | |
| erc20-transferfrom-correct-allowance | True | |
| erc20-transferfrom-fail-recipient-overflow | Inconclusive | |
| erc20-transferfrom-false | True | |
| erc20-transferfrom-never-return-false | True | |
| erc20-transferfrom-revert-zero-argument | True | |
| erc20-transferfrom-fail-exceed-balance | True | |

Detailed Results for Function `allowance`

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

Detailed Results for Function `transfer`

| Property Name | Final Result | Remarks |
|---|---|---|
| erc20-transfer-correct-amount | True | |
| erc20-transfer-recipient-overflow | Inconclusive | |
| erc20-transfer-false | True | |
| erc20-transfer-never-return-false | True | |
| erc20-transfer-revert-zero | True | |
| erc20-transfer-exceed-balance | True | |

Detailed Results for Function `approve`

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

Detailed Results for Function `totalSupply`

| Property Name | Final Result | Remarks |
|---|---|---|
| erc20-totalsupply-correct-value | True | |
| erc20-totalsupply-succeed-always | 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 | |

# APPENDIX | GENEX

## Finding Categories

| Categories | Description |
| --- | --- |
| Coding Style | Coding Style findings may not affect code behavior, but indicate areas where coding practices can be improved to make the code more understandable and maintainable. |
| Language Version | Language Version findings indicate that the code uses certain compiler versions or language features with known security issues. |
| Coding Issue | Coding Issue findings are about general code quality including, but not limited to, coding mistakes, compile errors, and performance issues. |
| Logical Issue | Logical Issue findings indicate general implementation issues related to the program logic. |
| Centralization | Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code. |

## 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. Each such contract was compiled into a mathematical model that 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.

The following assumptions and simplifications apply to our model:

- 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 specifications

All properties are expressed in a behavioral interface specification language that CertiK has developed for Solidity, which allows us to specify the behavior of each function in terms of the contract state and its parameters and return values, as well as contract properties that are maintained by every observable state transition. Observable state transitions occur when the

contract's external interface is invoked and the invocation does not revert, and when the contract's Ether balance is changed by the EVM due to another contract's "self-destruct" invocation. The specification language has the usual Boolean connectives, as well as the operator `\old` (used to denote the state of a variable before a state transition), and several types of specification clause:

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

- `requires [cond]` - the condition `cond`, which refers to a function's parameters, return values, and contract state variables, must hold when a function is invoked in order for it to exhibit a specified behavior.
- `ensures [cond]` - the condition `cond`, which refers to a function's parameters, return values, and both `\old` and current contract state variables, is guaranteed to hold when a function returns if the corresponding requires condition held when it was invoked.
- `invariant [cond]` - the condition `cond`, which refers only to contract state variables, is guaranteed to hold at every observable contract state.
- `constraint [cond]` - the condition `cond`, which refers to both `\old` and current contract state variables, is guaranteed to hold at every observable contract state except for the initial state after construction (because there is no previous state); constraints are used to restrict how contract state can change over time.

## Description of the Analyzed ERC-20 Properties

### Properties related to function `transferFrom`

#### erc20-transferfrom-correct-allowance

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:

```
ensures \result ==> allowance(\old(sender), msg.sender) == \old(allowance(sender,
msg.sender)) - \old(amount)
                  || (allowance(\old(sender), msg.sender) == \old(allowance(sender,
msg.sender)) && \old(allowance(sender, msg.sender)) == type(uint256).max);
```

#### erc20-transferfrom-correct-amount

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:

```
requires recipient != sender;
requires balanceOf(recipient) + amount <= type(uint256).max;
ensures \result ==> balanceOf(\old(recipient)) == \old(balanceOf(recipient) +
amount)
                  && balanceOf(\old(sender)) == \old(balanceOf(sender) - amount);
  also
requires recipient == sender;
ensures \result ==> balanceOf(\old(recipient)) == \old(balanceOf(recipient));
```

#### erc20-transferfrom-fail-exceed-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:

```
requires msg.sender != sender;
requires amount > allowance(sender, msg.sender);
ensures !\result;
```

#### erc20-transferfrom-fail-exceed-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:

```
requires amount > balanceOf(sender);
ensures !\result;
```

#### erc20-transferfrom-fail-recipient-overflow

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:

```
requires recipient != sender;
requires balanceOf(recipient) + amount > type(uint256).max;
ensures !\result;
```

#### erc20-transferfrom-false

If `transferFrom` returns `false` to signal a failure, it must undo all incurred state changes before returning to the caller.

Specification:

```
ensures !\result ==> \assigned (\nothing);
```

#### erc20-transferfrom-never-return-false

The `transferFrom` function must never return `false`.

Specification:

```
ensures \result;
```

#### erc20-transferfrom-revert-zero-argument

All calls of the form `transferFrom(from, dest, amount)` must fail for transfers from or to the zero address.

Specification:

```
ensures \old(sender) == address(0) ==> !\result;
also
ensures \old(recipient) == address(0) ==> !\result;
```

### Properties related to function `allowance`

#### erc20-allowance-change-state

Function `allowance` must not change any of the contract's state variables.

Specification:

```
assignable \nothing;
```

#### erc20-allowance-correct-value

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

Specification:

```
ensures \result == allowance(\old(owner), \old(spender));
```

#### erc20-allowance-succeed-always

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

Specification:

```
reverts_only_when false;
```

**Properties related to function `transfer`**

**erc20-transfer-correct-amount**

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:

```
requires recipient != msg.sender;
requires balanceOf(recipient) + amount <= type(uint256).max;
ensures \result ==> balanceOf(recipient) == \old(balanceOf(recipient) + amount)
&& balanceOf(msg.sender) == \old(balanceOf(msg.sender) - amount);
  also
requires recipient == msg.sender;
ensures \result ==> balanceOf(msg.sender) == \old(balanceOf(msg.sender));
```

**erc20-transfer-exceed-balance**

Any transfer of an amount of tokens that exceeds the balance of `msg.sender` must fail.

Specification:

```
requires amount > balanceOf(msg.sender);
ensures !\result;
```

**erc20-transfer-false**

If the `transfer` function in contract `GENEX` fails by returning `false`, it must undo all state changes it incurred before returning to the caller.

Specification:

```
ensures !\result ==> \assigned (\nothing);
```

**erc20-transfer-never-return-false**

The transfer function must never return `false` to signal a failure.

Specification:

```
ensures \result;
```

**erc20-transfer-recipient-overflow**

Any invocation of `transfer(recipient, amount)` must fail if it causes the balance of the `recipient` address to overflow.

Specification:

```
requires recipient != msg.sender;
requires balanceOf(recipient) + amount > type(uint256).max;
ensures !\result;
```

#### erc20-transfer-revert-zero

Any call of the form `transfer(recipient, amount)` must fail if the recipient address is the zero address.

Specification:

```
ensures \old(recipient) == address(0) ==> !\result;
```

### Properties related to function `approve`

#### erc20-approve-correct-amount

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:

```
requires spender != address(0);
ensures \result ==> allowance(msg.sender, \old(spender)) == \old(amount);
```

#### erc20-approve-false

If function `approve` returns `false` to signal a failure, it must undo all state changes that it incurred before returning to the caller.

Specification:

```
ensures !\result ==> \assigned (\nothing);
```

#### erc20-approve-never-return-false

The function `approve` must never returns `false`.

Specification:

```
ensures \result;
```

#### erc20-approve-revert-zero

All calls of the form `approve(spender, amount)` must fail if the address in `spender` is the zero address.

Specification:

```
ensures \old(spender) == address(0) ==> !\result;
```

#### erc20-approve-succeed-normal

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:

```
requires spender != address(0);
ensures \result;
reverts_only_when false;
```

### Properties related to function `totalSupply`

#### erc20-totalsupply-change-state

The `totalSupply` function in contract GENEX must not change any state variables.

Specification:

```
assignable \nothing;
```

#### erc20-totalsupply-correct-value

The `totalSupply` function must return the value that is held in the corresponding state variable of contract GENEX.

Specification:

```
ensures \result == totalSupply();
```

#### erc20-totalsupply-succeed-always

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

Specification:

```
reverts_only_when false;
```

### Properties related to function `balanceOf`

**erc20-balanceof-change-state**

Function `balanceOf` must not change any of the contract's state variables.

Specification:

```
assignable \nothing;
```

**erc20-balanceof-correct-value**

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

Specification:

```
ensures \result == balanceOf(\old(account));
```

**erc20-balanceof-succeed-always**

Function `balanceOf` must always succeed if it does not run out of gas.

Specification:

```
reverts_only_when false;
```

# 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.