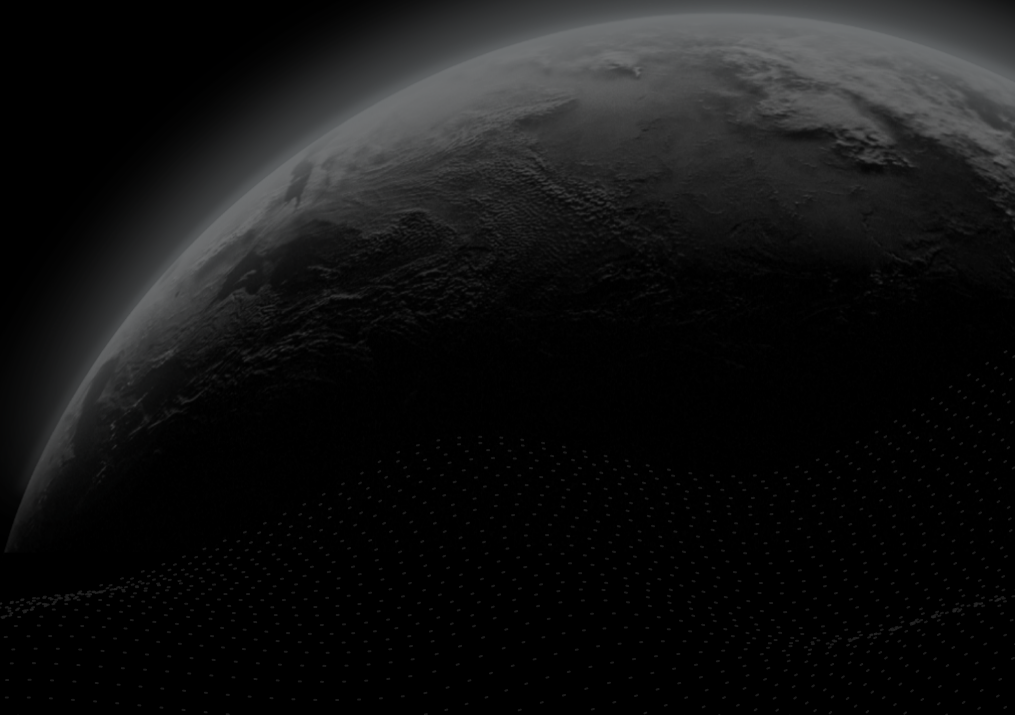




Security Assessment

Snark Launch

CertiK Verified on Apr 17th, 2023





CertiK Verified on Apr 17th, 2023

Snark Launch

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

Executive Summary

TYPES

DeFi

ECOSYSTEM

zkSync Era

METHODS

Formal Verification, Manual Review, Static Analysis

LANGUAGE

Solidity

TIMELINE

Delivered on 04/17/2023

KEY COMPONENTS

N/A

CODEBASE

<https://explorer.zksync.io/address/0x3Eb6b6B344a7Af4bab64210Ea64F19d7C2cC58fF#contract>

<https://explorer.zksync.io/address/0x533b5F887383196C6bc642f83338>

[...View All](#)

Vulnerability Summary



3

Total Findings

1

Resolved

1

Mitigated

1

Partially Resolved

0

Acknowledged

0

Declined

0

Unresolved

0 Critical

Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.

1 Major

1 Mitigated



Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.

0 Medium

Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.

0 Minor

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

1 Resolved, 1 Partially Resolved



Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | SNARK LAUNCH

I **Summary**

[Executive Summary](#)

[Vulnerability Summary](#)

[Codebase](#)

[Audit Scope](#)

[Approach & Methods](#)

I **Decentralization Efforts**

[Description](#)

[Recommendations](#)

I **Findings**

[STS-02 : Initial Token Distribution](#)

[STS-03 : Missing Emit Events](#)

[STS-04 : It is better to use a proxy_pattern](#)

I **Optimizations**

[ERC-01 : Proper usage of “pure” and “view”](#)

[SLC-01 : State Variable Should Be Declared Constant](#)

[SPS-01 : Variables That Could Be Declared as Immutable](#)

[STS-01 : Unused State Variable](#)

I **Formal Verification**

[Considered Functions And Scope](#)

[Verification Results](#)

I **Appendix**

I **Disclaimer**

CODEBASE | SNARK LAUNCH







■ Repository

<https://explorer.zksync.io/address/0x3Eb6b6B344a7Af4bab64210Ea64F19d7C2cC58fF#contract>

<https://explorer.zksync.io/address/0x533b5F887383196C6bc642f83338a69596465307#contract>

AUDIT SCOPE | SNARK LAUNCH

6 files audited ● 1 file with Acknowledged findings ● 1 file with Mitigated findings ● 1 file with Resolved findings
● 3 files without findings

ID	File	SHA256 Checksum
● ERC	 ERC20.sol	bce14c3fd3b1a668529e375f6b70ffdf9cef8c4e410ae99608be5964d98fa701
● STS	 SnrkToken.sol	af98e52ee3a39a599c5132062cb784914d6f71b783634d143c6db3ad38f65fc9
● SPS	 SnrkPrivate.sol	c40cfa9bf845eadecf5118d404337b0ae94583c4c8c76ab4da57196803c93f1e
● CSL	 Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
● IER	 IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db8003d075c9c541019eb8dcf4122864d5
● IEC	 IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990

APPROACH & METHODS | SNARK LAUNCH

This report has been prepared for Snark Launch to discover issues and vulnerabilities in the source code of the Snark Launch 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.

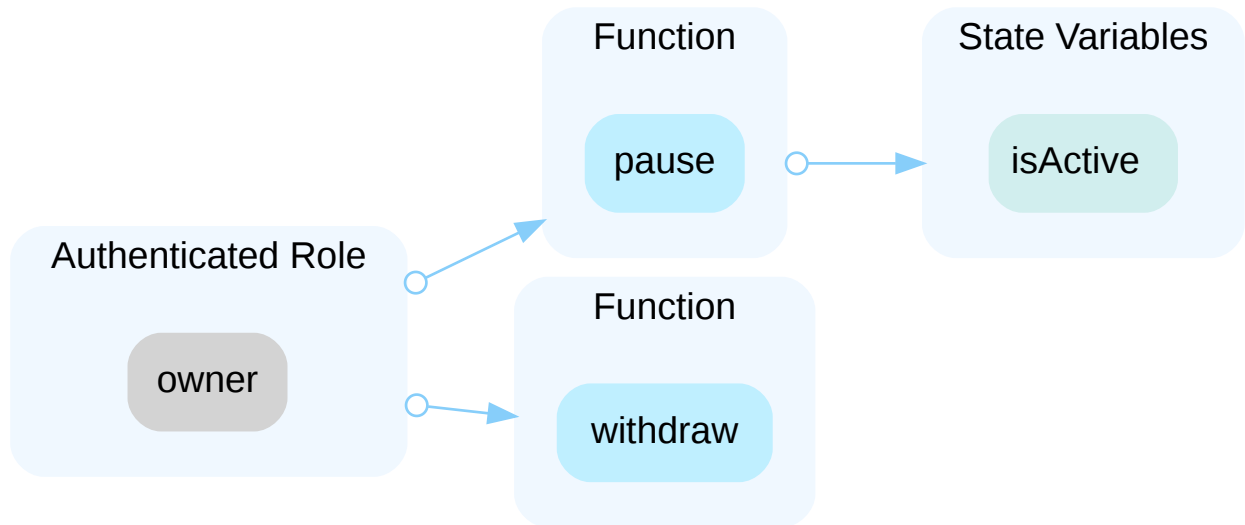
The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- 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.

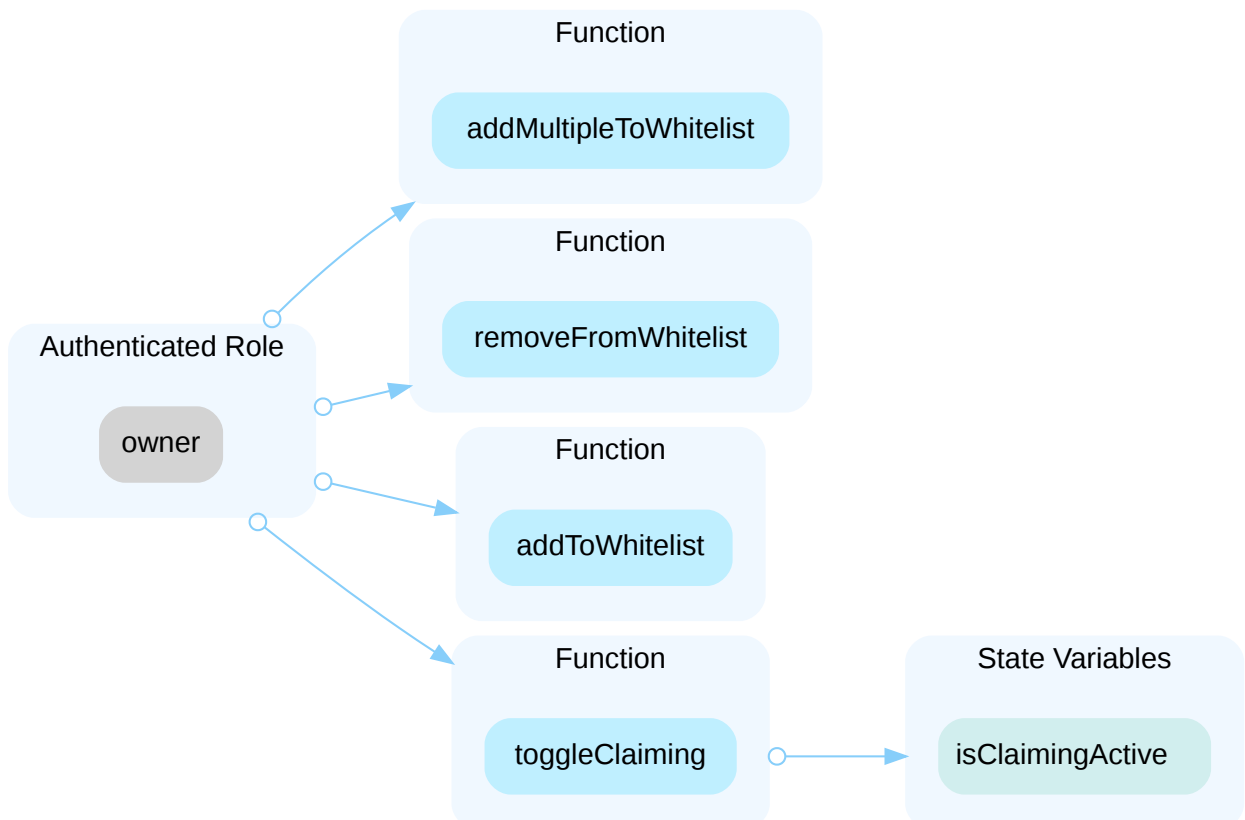
DECENTRALIZATION EFFORTS | SNARK LAUNCH

Description

In the contract `SnrkPrivate` 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.



In the contract `SnarkLaunch` 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.



Recommendations

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 ($\frac{2}{3}$, $\frac{3}{5}$) 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.

FINDINGS | SNARK LAUNCH



3

Total Findings

0

Critical

1

Major

0

Medium

0

Minor

2

Informational

This report has been prepared to discover issues and vulnerabilities for Snark Launch. Through this audit, we have uncovered 3 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
STS-02	Initial Token Distribution	Centralization / Privilege	Major	● Mitigated
STS-03	Missing Emit Events	Coding Style	Informational	● Resolved
STS-04	It Is Better To Use A Proxy Pattern	Language Specific, Volatile Code	Informational	● Partially Resolved

STS-02 | INITIAL TOKEN DISTRIBUTION

Category	Severity	Location	Status
Centralization / Privilege	● Major	SnrkToken.sol: 22	● Mitigated

I Description

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

I 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.

I Alleviation

The team published the token distribution plan:

<https://snark-launch.gitbook.io/snark-launch/tokenomics>

STS-03 | MISSING EMIT EVENTS

Category	Severity	Location	Status
Coding Style	● Informational	SnrkToken.sol: 26	● Resolved

Description

Functions that update state variables should emit relevant events as notifications.

Recommendation

We recommend adding events for state-changing actions, and emitting them in their relevant functions.

Alleviation

The team heeded our advice and resolved the issue in commit [232426afb184e80db9e7764090e3e2e1871d](#).

STS-04 | IT IS BETTER TO USE A PROXY PATTERN

Category	Severity	Location	Status
Language Specific, Volatile Code	● Informational	SnrkToken.sol	● Partially Resolved

Description

It's recommended to use the proxy pattern by the zkSync.

<https://era.zksync.io/docs/dev/building-on-zksync/contracts/differences-with-ethereum.html#recommendations>

Recommendation

We recommend to use proxy pattern to avoid some potential uncovered platform issues.

Alleviation

[Snark Launch] :

The contract currently doesn't have a hardcoded gas limit to avoid conflict with the chain. Additional tests will be done to avoid issues.

OPTIMIZATIONS | SNARK LAUNCH

ID	Title	Category	Severity	Status
ERC-01	Proper Usage Of "Pure" And "View"	Coding Style, Language Specific	Optimization	● Acknowledged
SLC-01	State Variable Should Be Declared Constant	Gas Optimization	Optimization	● Resolved
SPS-01	Variables That Could Be Declared As Immutable	Gas Optimization	Optimization	● Resolved
STS-01	Unused State Variable	Gas Optimization	Optimization	● Resolved

ERC-01 | PROPER USAGE OF “PURE” AND “VIEW”

Category	Severity	Location	Status
Coding Style, Language Specific	● Optimization	ERC20.sol: 87	● Acknowledged

Description

Function state mutability can be restricted to pure, functions can be declared pure in which case they promise not to read from or modify the state.

Recommendation

Consider declaring this function as pure.

Alleviation

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

SLC-01 | STATE VARIABLE SHOULD BE DECLARED CONSTANT

Category	Severity	Location	Status
Gas Optimization	● Optimization	SnrkPrivate.sol: 21; SnrkToken.sol: 15, 16	● Resolved

Description

State variables that never change should be declared as `constant` to save gas.

```
21     address public recipient = 0xEab8573343887E16efCfc6bD9C31b4f28e80ba84;
```

- `recipient` should be declared `constant` .

```
15     address public recipient;
```

- `recipient` should be declared `constant` .

```
16     uint256 percentage;
```

- `percentage` should be declared `constant` .

Recommendation

We recommend adding the `constant` attribute to state variables that never change.

Alleviation

The team heeded our advice and resolved the issue in commit [232426afbbf184e80dbeb9e7764090e3e2e1871d](#).

SPS-01 | VARIABLES THAT COULD BE DECLARED AS IMMUTABLE

Category	Severity	Location	Status
Gas Optimization	● Optimization	SnrkPrivate.sol: 22	● Resolved

Description

The linked variables assigned in the constructor can be declared as `immutable`. Immutable state variables can be assigned during contract creation but will remain constant throughout the lifetime of a deployed contract. A big advantage of immutable variables is that reading them is significantly cheaper than reading from regular state variables since they will not be stored in storage.

Recommendation

We recommend declaring these variables as immutable. Please note that the `immutable` keyword only works in Solidity version `v0.6.5` and up.

Alleviation

The team heeded our advice and resolved the issue in commit [232426afbfb184e80dbeb9e7764090e3e2e1871d](#).

STS-01 | UNUSED STATE VARIABLE

Category	Severity	Location	Status
Gas Optimization	● Optimization	SnrkToken.sol: 16	● Resolved

Description

One or more state variables are never used in the codebase.

Variable `percentage` in `SnarkLaunch` is never used in `SnarkLaunch`.

```
16     uint256 percentage;
```

```
7  contract SnarkLaunch is ERC20 {
```

Recommendation

We advise removing the unused variables.

Alleviation

The team heeded our advice and resolved the issue in commit [232426afb184e80db9e7764090e3e2e1871d](#).

FORMAL VERIFICATION | SNARK LAUNCH

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-succeed-normal	<code>transfer</code>	Succeeds on Admissible Non-self Transfers
erc20-transfer-revert-zero	<code>transfer</code>	Prevents Transfers to the Zero Address
erc20-transfer-succeed-self	<code>transfer</code>	Succeeds on Admissible Self Transfers
erc20-transfer-correct-amount	<code>transfer</code>	Transfers the Correct Amount in Non-self Transfers
erc20-transfer-correct-amount-self	<code>transfer</code>	Transfers the Correct Amount in Self Transfers
erc20-transfer-change-state	<code>transfer</code>	Has No Unexpected State Changes
erc20-transfer-exceed-balance	<code>transfer</code>	Fails if Requested Amount Exceeds Available Balance
erc20-transfer-recipient-overflow	<code>transfer</code>	Prevents Overflows in the Recipient's Balance
erc20-transfer-false	If <code>transfer</code>	Returns <code>false</code> , the Contract State Is Not Changed
erc20-transferfrom-revert-from-zero	<code>transferFrom</code>	Fails for Transfers From the Zero Address

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

For the following contracts, model checking established that each of the properties that were in scope of this audit (see scope) are valid:

Detailed Results For Contract SnarkLaunch (projects/SnarkLaunch/SnrkToken.sol) In Commit 386049f804f0aaebe83008cec7079e897a733ef3

Verification of ERC-20 Compliance

Detailed results for function transfer

Property Name	Final Result	Remarks
erc20-transfer-succeed-normal	● True	
erc20-transfer-revert-zero	● True	
erc20-transfer-succeed-self	● True	
erc20-transfer-correct-amount	● True	
erc20-transfer-correct-amount-self	● True	
erc20-transfer-change-state	● True	
erc20-transfer-exceed-balance	● True	
erc20-transfer-recipient-overflow	● True	
erc20-transfer-false	● True	
erc20-transfer-never-return-false	● True	

Detailed results for function `transferFrom`

Property Name	Final Result	Remarks
erc20-transferfrom-revert-from-zero	● True	
erc20-transferfrom-revert-to-zero	● True	
erc20-transferfrom-succeed-normal	● True	
erc20-transferfrom-correct-amount	● True	
erc20-transferfrom-correct-amount-self	● True	
erc20-transferfrom-succeed-self	● True	
erc20-transferfrom-fail-exceed-balance	● True	
erc20-transferfrom-correct-allowance	● True	
erc20-transferfrom-fail-exceed-allowance	● True	
erc20-transferfrom-change-state	● True	
erc20-transferfrom-never-return-false	● True	
erc20-transferfrom-fail-recipient-overflow	● True	
erc20-transferfrom-false	● True	

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	

APPENDIX | SNARK LAUNCH

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.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.
Language Specific	Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of private or delete.
Coding Style	Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

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 \Box) and "eventually" (written \Diamond), 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

recipient

```

[])(willSucceed(contract.transfer(to, value), to != msg.sender && _balances[to] >= 0
    && value >= 0 && _balances[to] + value <
    0x10000000000000000000000000000000000000000000000000000000000000000 &&
    _balances[msg.sender] >= 0 && _balances[msg.sender] <
    0x1000000000000000000000000000000000000000000000000000000000000000) ==>
<>(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

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

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

balance of `msg.sender`

```

[](started(contract.transfer(to, value), value > _balances[msg.sender] &&
    _balances[msg.sender] >= 0 && value <
    0x1000000000000000000000000000000000000000000000000000000000000000) ==>
<>(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:

[illegible]

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 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 <
    0x1000000000000000000000000000000000000000000000000000000000000000) ==>
<> (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] <  
        0x1000000000000000000000000000000000000000000000000000000000000000) ==>  
<>(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:

[illegible]

`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:

erc20-transferfrom-false

erc20-transferfrom-never-return-false

Properties related to function `totalSupply`

erc20-totalsupply-change-state

`totalSupply` Does Not Change the Contract's State. The `totalSupply` function in 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 <
    0x1000000000000000000000000000000000000000000000000000000000000000) ==>
    <> (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)))

```

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.



