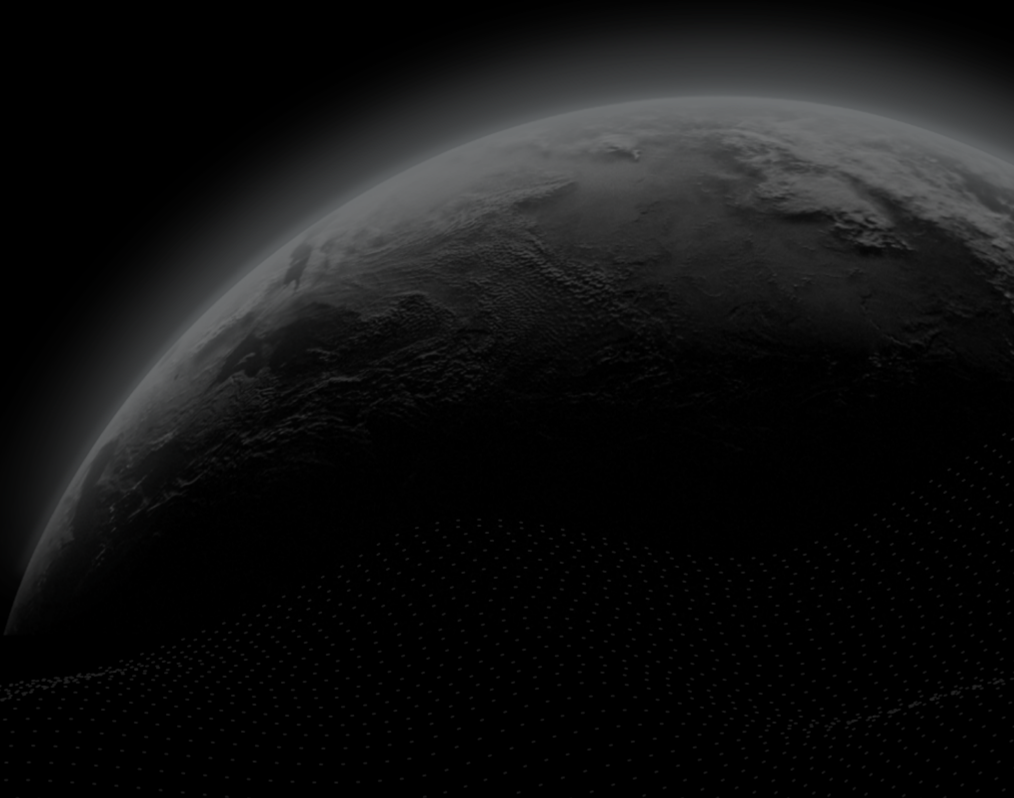
Security Assessment

REBorn

CertiK Verified on Apr 19th, 2023



CertiK Verified on Apr 19th, 2023

REBorn

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

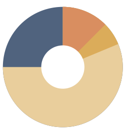
LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 04/19/2023	N/A

CODEBASE

https://bscscan.com/address/0x441bb79f2da0daf457bad3d401edb68535fb3faa

...View All

Vulnerability Summary



16	0	2	0	14	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	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.
2	Major	2 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.
1	Medium	1 Acknowledged	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
9	Minor	9 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.
4	Informational	4 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 | REBORN

CODEBASE | REBORN

Repository

https://bscscan.com/address/0x441bb79f2da0daf457bad3d401edb68535fb3faa

AUDIT SCOPE | REBORN

1 file audited ● 1 file with Acknowledged findings

ID	File	SHA256 Checksum
● HRC	HeyReborn.sol	e66348dfe43ae990ec813d3d66e56b4724e87a924bbc53afc176db0b60eca794

APPROACH & METHODS | REBORN

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

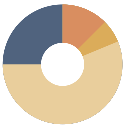
The auditing process pays special attention to the following considerations:

- 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 | REBORN



16	0	2	1	9	4
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for REBorn. Through this audit, we have uncovered 16 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
GLOBAL-01	**Initial Token Distribution**	**Centralization / Privilege**	**Major**	**Mitigated**
HRC-01	**Centralization Risks In HeyReborn.Sol**	**Centralization / Privilege**	**Major**	**Mitigated**
GLOBAL-02	`includeInReward()` Sets Balance To 0	Logical Issue	Medium	Acknowledged
HRC-02	Missing Zero Address Validation	Volatile Code	Minor	Acknowledged
HRC-03	Divide Before Multiply	Mathematical Operations	Minor	Acknowledged
HRC-04	Unused Return Value	Volatile Code	Minor	Acknowledged
HRC-05	Usage Of `transfer` / `send` For Sending Ether	Volatile Code	Minor	Acknowledged
HRC-06	Pontential Ineffective Function	Logical Issue	Minor	Acknowledged
HRC-07	Third Party Dependency	Volatile Code	Minor	Acknowledged
HRC-08	Potential Sandwich Attacks	Logical Issue	Minor	Acknowledged
HRC-09	Pull-Over-Push Pattern In `transferOwnership()` Function	Logical Issue	Minor	Acknowledged

ID	Title	Category	Severity	Status
HRC-10	Previous Owner Rights Are Not Revoked After Ownership Transfer	Logical Issue	Minor	Acknowledged
HRC-14	Unused `private` Function	Volatile Code	Informational	Acknowledged
HRC-21	Unlocked Compiler Version	Language Specific	Informational	Acknowledged
HRC-22	Inconsistent NatSpec For `transfer()` And `transferFrom()`	Inconsistency	Informational	Acknowledged
HRC-23	Too Many Digits	Coding Style	Informational	Acknowledged

GLOBAL-01 | INITIAL TOKEN DISTRIBUTION

Category	Severity	Location	Status
Centralization / Privilege	Major		Mitigated

Description

All `Hey Reborn` tokens are sent to the contract deployer when deploying the contract. This is a potential centralization risk as the deployer can distribute `Hey Reborn` 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

[Reborn Team]:

While all tokens were sent to deployer wallet upon deployment, we have actually deployed non-custodial vesting, multisig safe, and token distribution schedules.

You can check our token allocation, distribution, vesting/unlock schedules here on our whitepaper: https://re-born.gitbook.io/hey-re-born-whitepaper-2.0/hey-re-born-project/token-economics/token-distribution-and-token-allocation

We are using Superfluid platform to stream the wrapped RB tokens to our private sale investors, and wallets of each allocated categories. Unwrapping tokens can be done on Superfluid platform too.

This is contract of the wrapped token, deployed via the Superfluid platform: https://bscscan.com/address/0x744786ab00ed5a0b77ca754eb6f3ec0607c7fa79

Apart from TGE unlocked tokens (5.15 million), the rest of tokens are wrapped (using Superfluid platform), and stored in a multi-sig safe deployed on BSC (0x6Da78193edD3A824E073a81A9CDf1E4ae3d641b3) via Gnosis.

As we are using Superfluid vesting platform, this is their vesting smart contract:

https://bscscan.com/address/0x9b91c27f78376383003c6a12ad12b341d016c5b9

Here is Google Sheet with addresses for each allocations + private sales, and links for Superfluid Vesting page for each:

https://docs.google.com/spreadsheets/d/1I8cAMVeJfcqPnoltwMFWgRetjRNNBfavXeCgpb99hTg/edit?usp=sharing

HRC-01 | CENTRALIZATION RISKS IN HEYREBORN.SOL

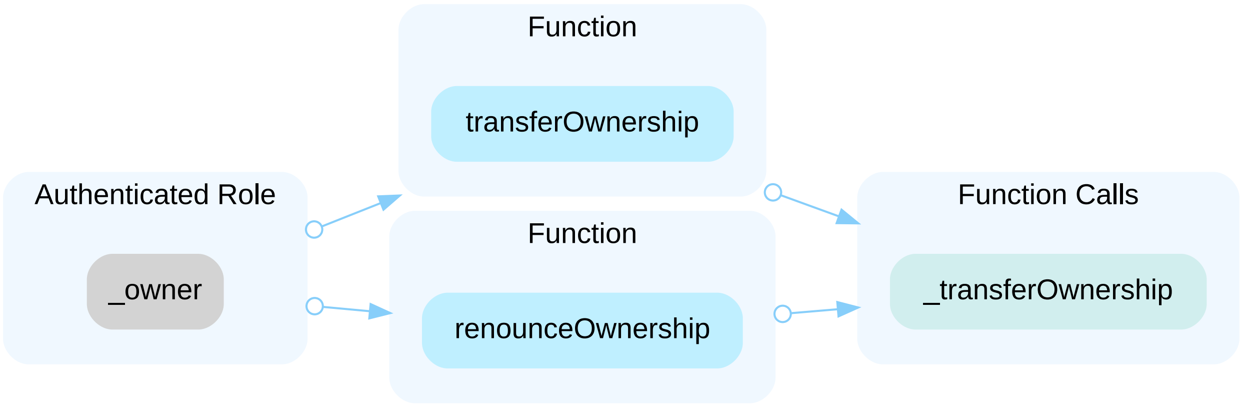
Category	Severity	Location	Status
Centralization / Privilege	**Major**	**HeyReborn.sol: 79, 87, 959, 971, 983, 992, 1005, 1017, 1021, 1025, 1029, 1034, 1128, 1139, 1145, 1158**	**Mitigated**

Description

In the contract `HeyReborn` 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 perform actions such as pause the contract and change the fee settings.


State Variables
pancakeswapV2Router
pancakeswapV2Pair
routerAddress
Function Calls
IPancakeRouter02
Function
setRouterAddress
Function Calls
IPancakeswapV2Factory
Function
createLiquidityPoolPair
State Variables
pancakeswapV2Router
pancakeswapV2Pair
isPairCreated
Function
setLiquidityPoolBuyFee
State Variables
_buyFee
Function
setTxFee
State Variables
txFee
Function
removeLiquidity
Function Calls
owner
Function
withdraw
Function Calls
payable
Function
burn
Function Calls
_burn
Authenticated Role
_owner
Function
setLiquidityFee
State Variables
liquidityFee
Function
unpause
State Variables
_paused
Function
setSwapAndLiquifyEnabled
State Variables
swapAndLiquifyEnabled
Function
includeInReward
Function
setLiquidityPoolSellFee
State Variables
_sellFee
Function
excludeFromReward
Function
pause
State Variables
_paused

In the contract `Ownable` 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 or renounce the ownership of 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 ($\frac{2}{3}$, $\frac{3}{5}$) 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.

Alleviation

[Reborn Team]:

We have deployed TimeLock contract using OpenZeppelin Defender, and Multisig via Defender too.

Hey Reborn smart contract is now owned by TimeLock Smart Contract (https://bscscan.com/address/0xF95b43E052404c0456994355B7AC981DD892F49d). TimeLock smart contract has only RB Controller (name of multisig) as both Proposer and Executer. TimeLock has minimum period of 48 hours/2 days. Execution Strategy for functions on Hey Reborn smart contract is using a combination of both RB Controller (Multis) and Timelock Contract. Any new actions can be Proposed and signed only by 2 signers out of 5 owner wallets of the multisig, and Executed by 2 signers out of 5 of the multisig too.

We will also be announcing this on our whitepaper. Centralization Mitigation Info

Multi-signature

Platform: BSC

Multi-sign proxy address: https://bscscan.com/address/0x13C4c2b0714C99E58FaA92b3e4FbF095e12FAD5a

Transaction proof for transferring ownership to multi-signature proxy:

Internal multi-signature address:
https://bscscan.com/address/0xeb14AbfC78b22D55B45603BC85Dc5ffd15b10cec,https://bscscan.com/address/0xF87c80936DC56119C50Bb9c4e0C31063cAD8FB37,https://bscscan.com/address/0xC5dD77bb2e3e073B48f6676ebd0Cbd0A835D49Ee,https://bscscan.com/address/0x827511d8D518094ba246023bd6C6Cd57DefF969A,https://bscscan.com/address/0x58Bd010887b25Ce13EFaf63d98d4a4AB3C43eEdB

Time-lock

Time lock contract address: https://bscscan.com/address/0xF95b43E052404c0456994355B7AC981DD892F49d

Time lock owner transfer transaction hash:
https://bscscan.com/tx/0xf160ca842ebc216a55ba64a89727dc2e421acea59abd78a14ab726760c32e192

GLOBAL-02 | `includeInReward()` SETS BALANCE TO 0

Category	Severity	Location	Status
Logical Issue	Medium		Acknowledged

Description

When an account is included in the reward list through `includeInReward()`, the account's balance is set to 0. This could lead to loss of user's tokens. Also, note that a reward mechanism is not implemented.

Recommendation

We advise to revise the linked function.

Alleviation

[REBorn Team]: The account balance setting to 0 (for $RB token) is on purpose so that if there were any rewards prior to being included, it will reset.

Also while our initial business logic was to do reward mechanism through this smart contract, we have changed our business logic. We will do rewards to our platform users differently, through loyalty mechanism which we will be developing later. This function will not be in use.

HRC-02 | MISSING ZERO ADDRESS VALIDATION

Category	Severity	Location	Status
Volatile Code	Minor	HeyReborn.sol: 756, 757	Acknowledged

Description

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

```
756        marketingFundAddress = payable(_marketingFundAddress);
```

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

```
757        routerAddress = _routerAddress;
```

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

Recommendation

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

Alleviation

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version. We do not plan to frequently change this and currently it is not in use either.

HRC-03 | DIVIDE BEFORE MULTIPLY

Category	Severity	Location	Status
Mathematical Operations	Minor	HeyReborn.sol: 763	Acknowledged

Description

Performing integer division before multiplication truncates the low bits, losing the precision of calculation.

```
763        minLiquidityAmount = (_totalSupply * 2 / 10000) * 10 ** _decimals;
```

Recommendation

We recommend applying multiplication before division to avoid loss of precision.

Alleviation

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version.

HRC-04 | UNUSED RETURN VALUE

Category	Severity	Location	Status
Volatile Code	Minor	HeyReborn.sol: 1113~1120, 1129~1136	Acknowledged

Description

The return value of an external call is not stored in a local or state variable.

```
1113        pancakeswapV2Router.addLiquidityETH{value: _bnbTokenAmount}(
1114            address(this),
1115            _rbTokenAmount,
1116            0, // slippage is unavoidable
1117            0, // slippage is unavoidable
1118            owner(),
1119            block.timestamp
1120        );
```

```
1129        pancakeswapV2Router.removeLiquidityETH(
1130          address(this),
1131          _liquidityAmountToRemove,
1132          0,
1133          0,
1134          owner(),
1135          block.timestamp
1136          );
```

Recommendation

We recommend checking or using the return values of all external function calls.

Alleviation

[REBorn Team]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

HRC-05 | USAGE OF `transfer` / `send` FOR SENDING ETHER

Category	Severity	Location	Status
Volatile Code	Minor	HeyReborn.sol: 1161	Acknowledged

Description

It is not recommended to use Solidity's `transfer()` and `send()` functions for transferring Ether, since some contracts may not be able to receive the funds. Those functions forward only a fixed amount of gas (2300 specifically) and the receiving contracts may run out of gas before finishing the transfer. Also, EVM instructions' gas costs may increase in the future. Thus, some contracts that can receive now may stop working in the future due to the gas limitation.

```
1161        payable(msg.sender).transfer(_amount);
```

- `HeyReborn.withdraw` uses `transfer()`.

Recommendation

We recommend using the `Address.sendValue()` function from OpenZeppelin.

Since `Address.sendValue()` may allow reentrancy, we also recommend guarding against reentrancy attacks by utilizing the Checks-Effects-Interactions Pattern or applying OpenZeppelin ReentrancyGuard.

HRC-06 | PONTENTIAL INEFFECTIVE FUNCTION

Category	Severity	Location	Status
Logical Issue	Minor	HeyReborn.sol: 1005	Acknowledged

Description

The `createPair()` function reverts if the `$VARIABLE - WETH` pair already exists. So calling the `getPair()` function before calling the `createPair()` function is better choice.

Recommendation

We advise refactoring the linked statements as below:

```
address get_pair = IUniswapV2Factory(_uniswapV2Router.factory()).getPair(address(this), _uniswapV2Router.WETH());
if (get_pair == address(0)) {
    uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this), _uniswapV2Router.WETH());
} else {
    uniswapV2Pair = get_pair;
}
```

Alleviation

[REBorn Team]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

HRC-07 | THIRD PARTY DEPENDENCY

Category	Severity	Location	Status
Volatile Code	Minor	HeyReborn.sol: 1092, 1111, 1128	Acknowledged

Description

The contract is serving as the underlying entity to interact with third party `PancakeSwap` protocol. The scope of the audit treats 3rd party entities as black boxes and assume their functional correctness. However, in the real world, 3rd parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of 3rd parties can possibly create severe impacts, such as increasing fees of 3rd parties, migrating to new LP pools, etc.

Recommendation

We understand that the business logic of `REBorn` requires interaction with `PancakeSwap` . We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version. We will constantly monitor the status of PancakeSwap protocol for possible mitigations if and when necessary.

HRC-08 | POTENTIAL SANDWICH ATTACKS

Category	Severity	Location	Status
Logical Issue	Minor	HeyReborn.sol: 1097~1103, 1113~1120, 1129~1136	Acknowledged

Description

A sandwich attack may happen when an attacker observes a transaction swapping tokens or adding liquidity without setting restrictions on slippage or minimum output amount. The attacker can manipulate the exchange rate by front running (before the transaction being attacked) a transaction to purchase one of the assets and make profits by back running (after the transaction being attacked) a transaction to sell the asset.

The following functions are called without setting restrictions on slippage or minimum output amount, so transactions triggering these functions are vulnerable to sandwich attacks, especially when the input amount is large:

- `swapExactTokensForETHSupportingFeeOnTransferTokens()`
- `addLiquidityETH()`
- `removeLiquidityETH()`

Recommendation

We recommend setting reasonable minimum output amounts, instead of 0, based on token prices when calling the aforementioned functions.

Alleviation

[REBorn Team]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

HRC-09 | PULL-OVER-PUSH PATTERN IN `transferOwnership()` FUNCTION

Category	Severity	Location	Status
Logical Issue	Minor	HeyReborn.sol: 87	Acknowledged

Description

The change of `_owner` by function `transferOwnership()` overrides the previously set `_owner` with the new one without guaranteeing the new `_owner` is able to actuate transactions on-chain.

Recommendation

We advise the pull-over-push pattern to be applied here whereby a new `_owner` is first proposed and consequently needs to accept the `_owner` status ensuring that the account can actuate transactions on-chain. The following code snippet can be taken as a reference:

```
address public potentialAdmin;

function transferAdmin(address pendingAdmin) external onlyAdmin {
    require(pendingAdmin != address(0), "potential admin can not be the zero
address.")
    potentialAdmin = pendingAdmin;
    emit AdminNominated(pendingAdmin);
}

function acceptAdmin() external {
    require(msg.sender == potentialAdmin, 'You must be nominated as potential admin
before you can accept administer role');
    admin = potentialAdmin;
    potentialAdmin = address(0);
    emit AdminChanged(admin)
}
```

Alleviation

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version, as the ownership has already been transferred to another wallet (also owned and controlled by the foundation).

HRC-10 | PREVIOUS OWNER RIGHTS ARE NOT REVOKED AFTER OWNERSHIP TRANSFER

Category	Severity	Location	Status
Logical Issue	Minor	HeyReborn.sol: 87, 765	Acknowledged

Description

When the contract is deployed, the owner is excluded from the transfer fees. However, when the ownership is transferred, the fees are not restored for the old owner and excluded for the new one.

Recommendation

We advise to revise the linked function.

Alleviation

[REBorn Team]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

Additionally, previous owner wallet is also owned by the foundation. Plus, it does not hold any RB tokens so it is not a problem.

HRC-14 | UNUSED `private` FUNCTION

Category	Severity	Location	Status
Volatile Code	Informational	HeyReborn.sol: 1060, 1070	Acknowledged

Description

The functions `removeAllFee()` and `restoreAllFee()` are private functions never called within the contract. At no point in execution will `removeAllFee()` or `restoreAllFee()` be called.

Recommendation

We advise to remove the redundant statements for production environments.

Alleviation

[REBorn Team]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

HRC-21 | UNLOCKED COMPILER VERSION

Category	Severity	Location	Status
Language Specific	Informational	HeyReborn.sol: 5, 31, 107, 336, 400	Acknowledged

Description

The contracts cited have 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

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version.

HRC-22 INCONSISTENT NATSPEC FOR `transfer()` AND `transferFrom()`

Category	Severity	Location	Status
Inconsistency	Informational	HeyReborn.sol: 875, 890	Acknowledged

Description

The NatSpec of the functions `transfer()` and `transferFrom()` state that the `nonReentrant` modifier is used. However, this modifier is not used in the specified functions.

Recommendation

We recommend changing the code or the NatSpec to reflect the intended project design.

Alleviation

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version.

HRC-23 | TOO MANY DIGITS

Category	Severity	Location	Status
Coding Style	Informational	HeyReborn.sol: 754, 763, 1265	Acknowledged

Description

Literals with many digits are difficult to read and review.

Recommendation

We recommend using scientific notation (e.g. `1e6`) or underscores (e.g. `1_000_000`) to improve readability.

Alleviation

[Team REBorn]: Issue acknowledged. I won't make any changes for the current version.

OPTIMIZATIONS | REBORN

ID	Title	Category	Severity	Status
HRC-15	Unnecessary Use Of SafeMath	Gas Optimization	Optimization	Acknowledged
HRC-16	State Variable Should Be Declared Constant	Gas Optimization	Optimization	Acknowledged
HRC-17	Unused State Variable	Gas Optimization	Optimization	Acknowledged
HRC-18	Variables That Could Be Declared As Immutable	Gas Optimization	Optimization	Acknowledged
HRC-19	User-Defined Getters	Gas Optimization	Optimization	Acknowledged
HRC-20	Function Visibility Optimization	Gas Optimization	Optimization	Acknowledged

HRC-15 | UNNECESSARY USE OF SAFEMATH

Category	Severity	Location	Status
Gas Optimization	Optimization	HeyReborn.sol: 119, 767, 898, 933, 946, 1045~1047, 1051 ~1053, 1057, 1079, 1080, 1083, 1198, 1199, 1231, 1237, 1243, 1245, 1268, 1278, 1298, 1299, 1328	Acknowledged

Description

The `SafeMath` library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations will automatically revert in case of integer overflow or underflow.

```
119  library SafeMath {
```

- An implementation of `SafeMath` library is found.

```
686    using SafeMath for uint256;
```

- `SafeMath` library is used for `uint256` type in `HeyReborn` contract.

```
767        balances[msg.sender] = balances[msg.sender].add(_totalSupply);
```

- `SafeMath.add` is called in `constructor` function of `HeyReborn` contract.

Note: Only a sample of 2 `SafeMath` library usage in this contract (out of 26) are shown above.

Recommendation

We advise removing the usage of `SafeMath` library and using the built-in arithmetic operations provided by the Solidity programming language.

Alleviation

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version, as this is only for gas optimisation and does not create any problems/conflicts.

HRC-16 | STATE VARIABLE SHOULD BE DECLARED CONSTANT

Category	Severity	Location	Status
Gas Optimization	Optimization	HeyReborn.sol: 726, 727, 728	Acknowledged

Description

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

```
691    uint256 private _rTotal;
```

- `_rTotal` should be declared `constant`.

```
716    address payable private partnershipFundAddress;
```

- `partnershipFundAddress` should be declared `constant`.

```
717    address payable private airdropFundAddress;
```

- `airdropFundAddress` should be declared `constant`.

```
719    address payable private staffFundAddress;
```

- `staffFundAddress` should be declared `constant`.

```
720    address payable private burnFundAddress;
```

- `burnFundAddress` should be declared `constant`.

```
721    address payable private holdersFundAddress;
```

- `holdersFundAddress` should be declared `constant`.

```
address public pancakeFactory = 0xcA143Ce32Fe78f1f7019d7d551a6402fC5350c73;
```

- `pancakeFactory` should be declared `constant`.

```
address public pancakeRouterAddress = 0x10ED43C718714eb63d5aA57B78B54704E256024E;
```

- `pancakeRouterAddress` should be declared `constant`.

```
address public WETH = address(0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c); //WBNB
```

- `WETH` should be declared `constant`.

Recommendation

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

Alleviation

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version.

HRC-17 | UNUSED STATE VARIABLE

Category	Severity	Location	Status
Gas Optimization	Optimization	HeyReborn.sol: 691, 697, 716, 717, 719, 720, 721, 735	Acknowledged

Description

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

Variable `_rTotal` in `HeyReborn` is never used in `HeyReborn`.

```
691     uint256 private _rTotal;
```

```
685   contract HeyReborn is Ownable, IBEP2E,ReentrancyGuard {
```

Variable `_rOwned` in `HeyReborn` is never used in `HeyReborn`.

```
697     mapping (address => uint256) private _rOwned;
```

```
685   contract HeyReborn is Ownable, IBEP2E,ReentrancyGuard {
```

Variable `partnershipFundAddress` in `HeyReborn` is never used in `HeyReborn`.

```
716     address payable private partnershipFundAddress;
```

```
685   contract HeyReborn is Ownable, IBEP2E,ReentrancyGuard {
```

Variable `airdropFundAddress` in `HeyReborn` is never used in `HeyReborn`.

```
717     address payable private airdropFundAddress;
```

```
685   contract HeyReborn is Ownable, IBEP2E,ReentrancyGuard {
```

Variable `staffFundAddress` in `HeyReborn` is never used in `HeyReborn`.

```
719     address payable private staffFundAddress;
```

```
contract HeyReborn is Ownable, IBEP2E,ReentrancyGuard {
```

Variable `burnFundAddress` in `HeyReborn` is never used in `HeyReborn`.

```
    address payable private burnFundAddress;
```

```
contract HeyReborn is Ownable, IBEP2E,ReentrancyGuard {
```

Variable `holdersFundAddress` in `HeyReborn` is never used in `HeyReborn`.

```
    address payable private holdersFundAddress;
```

```
contract HeyReborn is Ownable, IBEP2E,ReentrancyGuard {
```

Variable `MAX` in `HeyReborn` is never used in `HeyReborn`.

```
    uint256 private constant MAX = ~uint256(0);
```

```
contract HeyReborn is Ownable, IBEP2E,ReentrancyGuard {
```

Recommendation

We advise removing the unused variables.

Alleviation

[REBorn Team]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

HRC-18 | VARIABLES THAT COULD BE DECLARED AS IMMUTABLE

Category	Severity	Location	Status
Gas Optimization	Optimization	HeyReborn.sol: 692, 718, 729, 733	Acknowledged

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

[REBorn Team]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

HRC-19 | USER-DEFINED GETTERS

Category	Severity	Location	Status
Gas Optimization	Optimization	HeyReborn.sol: 825~827, 833~835, 841~843	Acknowledged

Description

The linked functions are equivalent to the compiler-generated getter functions for the respective variables.

Recommendation

We advise that the linked variables are instead declared as `public` as compiler-generated getter functions are less prone to error and much more maintainable than manually written ones.

Alleviation

[REBorn Team]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

HRC-20 | FUNCTION VISIBILITY OPTIMIZATION

Category	Severity	Location	Status
Gas Optimization	Optimization	HeyReborn.sol: 79, 825, 833, 841, 849, 857, 880, 896, 909, 921, 932, 943, 959, 971, 983, 992, 1029, 1056, 1128, 1139, 1158	Acknowledged

Description

The following functions are declared as `public`, and are not invoked in any of the contracts contained within the project's scope. Functions that are never called internally within the contract should have `external` visibility.

Recommendation

We recommend setting visibility specifiers to `external`, optimising the gas cost of the function.

Alleviation

[REBorn Team]: Issue acknowledged. I won't make any changes for the current version.

FORMAL VERIFICATION | REBORN

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	`transfer` Succeeds on Admissible Non-self Transfers
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-change-state	`transfer` Has No Unexpected State Changes
erc20-transfer-correct-amount-self	`transfer` Transfers the Correct Amount in Self Transfers
erc20-transfer-recipient-overflow	`transfer` Prevents Overflows in the Recipient's Balance
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-transferfrom-revert-from-zero	`transferFrom` Fails for Transfers From the Zero Address

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

Property Name	Title
erc20-allowance-change-state	`allowance` Does Not Change the Contract's State
erc20-approve-correct-amount	`approve` Updates the Approval Mapping Correctly
erc20-approve-false	If `approve` Returns `false`, the Contract's State Is Unchanged
erc20-approve-succeed-normal	`approve` Succeeds for Admissible Inputs
erc20-approve-never-return-false	`approve` Never Returns `false`
erc20-approve-change-state	`approve` Has No Unexpected State Changes

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 HeyReborn (HeyReborn.sol) In Commit 0x441bb79f2da0daf457bad3d401edb68535fb3faa

Verification of ERC-20 Compliance

Detailed results for function `transfer`

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

Detailed results for function `transferFrom`

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

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-correct-amount	● True	
erc20-approve-false	● True	
erc20-approve-succeed-normal	● Inapplicable	Intended behavior
erc20-approve-never-return-false	● True	
erc20-approve-change-state	● True	

APPENDIX | REBORN

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.
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.
Inconsistency	Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different require statements on the input variables than a setter function.

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)))
```

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.