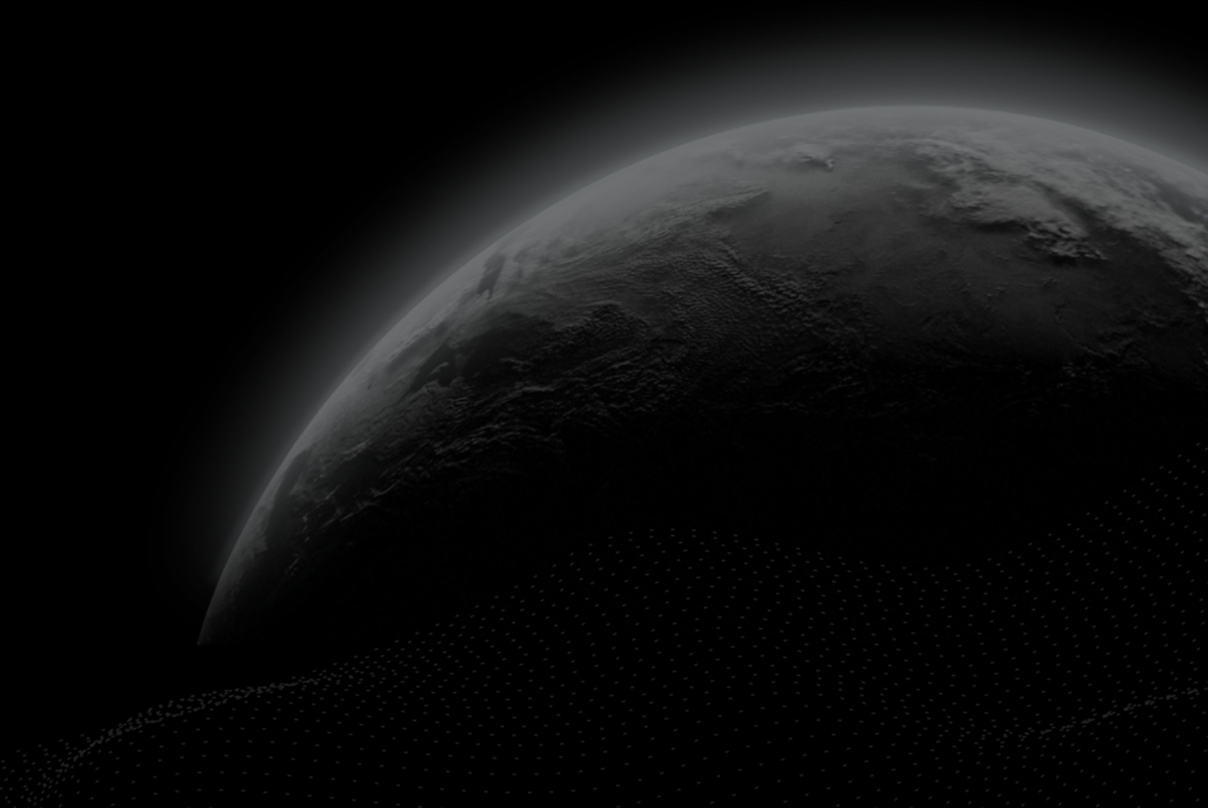
Economic Assessment

T.I.M.E. Dividend (TIME) - BNB Smart Chain (BSC)

CertiK Verified on Mar 24th, 2023



CertiK Verified on Mar 24th, 2023

T.I.M.E. Dividend (TIME) - BNB Smart Chain (BSC)

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

Executive Summary

TYPES
DeFi

ECOSYSTEM
Binance Smart Chain (BSC)

METHODS
Formal Verification, Manual Review

LANGUAGE
Solidity

TIMELINE
Delivered on 03/24/2023

KEY COMPONENTS
TIMEDividend

CODEBASE
https://bitbucket.org/internet-money/wallet-contracts/src/master/contracts/TIMEDividend.sol
...View All

COMMITS
856179395047c7818b0b34ddae503089ba0c2969
...View All

Vulnerability Summary

Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved
0	0	0	0	0	0	0

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

T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

CODEBASE | T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

Repository

https://bitbucket.org/internet-money/wallet-contracts/src/master/contracts/TIMEDividend.sol

Commit

856179395047c7818b0b34ddae503089ba0c2969

AUDIT SCOPE | T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

1 file audited ● 1 file without findings

ID	File	SHA256 Checksum
TIM	TIMEDividend.sol	bb0400ff9b904a7de218ab0039e6eb169d1d18e72d485eecc8b7dda25b07f52a

APPROACH & METHODS | T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

This report has been prepared for T.I.M.E. Dividend to discover issues and vulnerabilities of the economic model of the T.I.M.E. Dividend (TIME) - BNB Smart Chain (BSC) project, based on the source code of the T.I.M.E. Dividend (TIME) - BNB Smart Chain (BSC) project. We treated the provided background information (Appendix) as design specifications. A comprehensive examination has been performed, utilizing Manual Review techniques.

The auditing process includes the following considerations:

- Conducting rigorous mathematical reasoning to analyze the economic model, with particular emphasis on discrete data types, to ensure accuracy and reliability.
- Assessing the compliance of the economic model with current industry standards and best practices to identify areas for improvement.
- Reviewing the economic model to ensure the preservation of semantics in comparison to the design documentation, and that no essential elements have been lost.
- Performing a meticulous manual line-by-line review of the codebase to confirm that the code implementation aligns with the economic model and satisfies all applicable standards and requirements.

INTRODUCTION | T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

The `TIMEDividend` contract allows for the distribution of dividends to token holders. The dividends are paid out in native coins (BNB), with the amount distributed based on the number of tokens held by each address after delta correction. The delta correction moves opposite to the token flow of token transferring, such that in general, the dividend distribution is aligned with the initial token holding status. Generally we do not recommend the token distribution to have more than half of the total supply held by one user, given that the initial token distribution takes place before the contract is ready and allowed to work.

The contract uses a unique approach to calculate dividends, where `magnifiedDividendPerShare` and `magnifiedDividendCorrections` of each address are to ensure that the dividend payouts/claims are maintained over time.

A core value of the calculation if the state variable `magnitude`, which is a constant value used to convert amounts to scaling magnitudes. It used to maintaining the resolution of payouts to be accurately calculated for very small amounts. It is hardcoded to 2^{128} in the contract.

The contract contains two key mappings, `cumulativeDividendClaimed` and `magnifiedDividendCorrections`. `cumulativeDividendClaimed` is used to track the cumulative amount of dividend claimed by each address, ensuring that double payouts are not made. `magnifiedDividendCorrections` is used to track corrections made to the magnified dividend per share as tokens are transferred between accounts.

The `receive()` function is aim to receive fees generated from the swap operations, which is not implemented in the TIMEDividend contract. In fact the `receive` function does not specify which address is the source of the fees, such that it allows any addresses to send native coin (BNB) to itself. The function requires that the minting process is complete and the ownership has been renounced, which can also be seen as a status that the whole contract is ready to start functioning.

PROTOCOL DESCRIPTION | T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

State Variables

```
uint256 public constant magnitude = 2**128;
uint256 public magnifiedDividendPerShare;

mapping(address => int256) public magnifiedDividendCorrections;
mapping(address => uint256) public cumulativeDividendClaimed;
```

Functions

receive()

Let a_b be the native coins (BNB) transfer amount, which is also known as `msg.value` in Solidity. For each function call, we have

$$magnifiedDividendPerShare += \frac{a_b}{totalSupply} \times magnitude$$

If the receive function is called for n times, we have

$$magnifiedDividendPerShare_n = \sum_{i=1}^{n} \frac{a_{bi}}{totalSupply} \times magnitude$$

$$\implies magnifiedDividendPerShare_n = 2^{128} * \sum_{i=1}^{n} \frac{a_{bi}}{totalSupply}$$

where `totalSupply` cannot be increased since the require statement of the `receive` function checks that the contract ownership is already renounced.

_beforeTokenTransfer()

Let's say there is a transfer transaction, where u_s is the sender's address, u_r is the recepient address, and a_t is the token transfer amount. Let `magnifiedDividendCorrections` be mdc. If this function is called for n times, we have

$$mdc[u_s] = \sum_{i=1}^{n} magnifiedDividendPerShare \times a_t$$

and

$$mdc[u_r] = -\sum_{i=1}^{n} magnifiedDividendPerShare \times a_t$$

divideFrom()

$$product = magDividendPerShare * balance + correction$$

$$return_1 = product / magnitude$$

$$\implies return_1 = (magDividendPerShare * balance + correction) \div magnitude$$

$$return_2 = product \mod magnitude$$

$$\implies return_2 = (magDividendPerShare * balance + correction) \mod magnitude$$

accumulativeDividendOf()

Let `magnifiedDividendCorrections` be mdc, and `account` be the input address. Also since there are two parts of the return value, let the former value be $return_1$ and the latter value be $return_2$.

$$return_1 = product/magnitude$$

$$\implies return_1 = (magDividendPerShare * balanceOf(account) + mdc[account]) \div magnitude$$

$$return_2 = product \mod magnitude$$

$$\implies return_2 = (magDividendPerShare * balanceOf(account) + mdc[account]) \mod magnitude$$

claimableDividendOf()

Let `magnifiedDividendCorrections` be mdc, `account` be the input address, and `cumulativeDividendClaimed` be cdc, we have

$$return = (return_1\ of\ dividendFrom) - cdc[account]$$

$$\implies return = \frac{magDividendPerShare*balanceOf(account)+mdc[account]}{magnitude} - cdc[account]$$

claimDividend()

Let `magnifiedDividendCorrections` be mdc, and let `cumulativeDividendClaimed` be cdc.

$$claimable = \frac{magDividendPerShare*balanceOf(account)+mdc[account]}{magnitude} - cdc[account]_{old}$$

$$recipent\ balance += claimable \text{ , where currency BNB}$$

$$cdc[account] += claimable$$

distributeAll()

This function is removed in commit hash `d6c89e5dac14b6db95f9dc67af54bd76103805fe` .

~~Called function `distributeAll()` from interface `IInternetMoneySwapRouter` . The function sends all fees, the input `amount` of native coins and/or WETH tokens, to the `destination` address defined in the contract behind the `IInternetMoneySwapRouter` .~~

PROTOCOL ANALYSIS | T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

The smart contract and its functions don't maintain any time-related variables, so the length of time a user holds TIME tokens doesn't affect the final dividend amount. We thoroughly examined the state and local variables of the TIMEDividend contract and found that it doesn't store or use any external data related to a locking time period. Therefore, the only variables that influence a user's dividend/reward are the `magnifiedDividendPerShare`, the amount of TIME tokens held by the user's address, and the `magnifiedDividendCorrections` (mdc) of the user's address.

Claimable Dividend

Within the four state variables, `magnitude` is declared to be `constant`.

`magnifiedDividendPerShare` is a variable that keeps track of the magnified dividend per share. It is calculated by dividing the total amount of dividend received by the `<total supply of tokens>`, and then multiplying by `magnitude` (2^{128}).

The `magnifiedDividendCorrections` mapping keeps track of the magnified dividend corrections for each account. Magnified dividend corrections are used to adjust the claimable dividend of an account based on its transfer history.

The `cumulativeDividendClaimed` mapping keeps track of the cumulative dividend claimed for each account. It is used to calculate the total claimable dividend for an account.

Here we would like to summarize a general math expression of the claimable dividend of a user. For the n-th time the function `claimDividend` is being called by an address, define the follow variables:

- `msg.sender`, the function caller address: u
- `magnifiedDividendPerShare`: `mdps`
- the previous claimed dividend summation: cdc_{n-1}
- the number of function calls of `claimDividend` before this call : n_c
- the number of function calls of `receive` : n_{nc}
    - the received BNB amount of the i_{nc} time with the total n_{nc} time:$amount_{i_{nc}}$
- the number of function calls of `transfer` as a sender: n_{ts}
    - the sent token amount of the i_{ts} time with the total n_{ts} time: $amount_{i_{ts}}$
- the number of function calls of `transfer` as a receiver: n_{tr}
    - the received token amount of the i_{tr} time with the total n_{tr} time: $amount_{i_{tr}}$
- the number of function calls of `burn` : n_b
    - the burnt token amount of the i_b time with the total n_b time: $amount_{i_b}$
- initial token balance of the user: $initBal$

- current token balance of the user: $currBal$, at the n-th call of `claimDividend`

From the above function description, we have

$$claimable_n = \frac{magDividendPerShare_{n_{nc}} * balanceOf(account) + mdc[account]}{magnitude} - cdc_{old}$$

Here for the balance of u at the n-th call of `claimDividend`, the current token balance is

$$currBal = initBal - \text{<all sent amount>} + \text{<all received amount>} - \text{<all burnt amount>}$$

$$\implies currBal = initBal - \sum_{i_{ts}=1}^{n_{ts}} amount_{i_{tr}} + \sum_{i_{ts}=1}^{n_{tr}} amount_{i_{tr}} - \sum_{i_b=1}^{n_b} amount_{i_b}$$

Similarly, we have the `magnifiedDividendCorrections` be

$$mdc = mdps * (\text{<all sent amount>} - \text{<all received amount>} + \text{<all burnt amount>})$$

$$\implies mdc = mdps * (\sum_{i_{ts}=1}^{n_{ts}} amount_{i_{tr}} - \sum_{i_{ts}=1}^{n_{tr}} amount_{i_{tr}} + \sum_{i_b=1}^{n_b} amount_{i_b})$$

In the meanwhile, `magnifiedDividendPerShare` is monotonically increasing controlled by the `receive` function. From the above function description of `receive`, we have

$$magnifiedDividendPerShare_{n_{nc}} = \sum_{i_{nc}=1}^{n_{nc}} \frac{amount_{i_{nc}}}{totalSupply} \times magnitude$$

Also, for the previous claimed dividend summation, we have $cdc_{n-1} = \sum_{i=1}^{n-1} claimable_i$

Therefore, for $claimable_n$, we have

$$claimable_n = \frac{magDividendPerShare_{n_{nc}} * balanceOf(account) + mdc[account]}{magnitude} - cdc_{old}$$

Substitute the variable names and make them fit the latest definition in the analysis.

$$claimable_n = \frac{mdps_{n_{nc}} * currBal + mdc}{magnitude} - cdc_{n-1}$$

Since $mdc == mdps * (\text{<transfer amount delta>})$, we can extract $\frac{mdps}{magnitude}$, and then we have

$$claimable_n = \frac{mdps}{magnitude} * (currBal + \frac{mdc}{mdps}) - \sum_{i=1}^{n-1} claimable_i$$

Substitute $currBal$ and mdc, we have the expression with the detailed amount summation based on the times of different functions being called for the current `receiver` function caller.

$$\implies claimable_n = \frac{mdps}{magnitude} * (initBal - \sum_{i_{ts}=1}^{n_{ts}} amount_{i_{tr}} + \sum_{i_{ts}=1}^{n_{tr}} amount_{i_{tr}} - \sum_{i_b=1}^{n_b} amount_{i_b} + \sum_{i_{ts}=1}^{n_{ts}} amount_{i_{tr}} - \sum_{i_{ts}=1}^{n_{tr}} amount_{i_{tr}} + \sum_{i_b=1}^{n_b} amount_{i_b}) - \sum_{i=1}^{n-1} claimable_i$$

$$= \frac{mdps}{magnitude} * initBal - \sum_{i=1}^{n-1} claimable_i$$

$$= \frac{\sum_{i_{nc}=1}^{n_{nc}} \frac{amount_{i_{nc}}}{totalSupply} \times magnitude}{magnitude} - \sum_{i=1}^{n-1} claimable_i$$

$$= \sum_{i_{nc}=1}^{n_{nc}} \frac{amount_{i_{nc}}}{totalSupply} - \sum_{i=1}^{n-1} claimable_i$$

Here when $i = 1$, the base case gives that the $claimable_1 = 0$, and the first time claimable dividend is the sum of quotient of each native coin (BNB) deposit divided by the total supply at that time.

FORMAL VERIFICATION | T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

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

Considered Functions And Scope

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

Verification of ERC-20 Compliance

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

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

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

Property Name	Title
erc20-transfer-revert-zero	`transfer` Prevents Transfers to the Zero Address
erc20-transfer-succeed-self	`transfer` Succeeds on Admissible Self Transfers
erc20-transfer-succeed-normal	`transfer` Succeeds on Admissible Non-self Transfers
erc20-transfer-correct-amount	`transfer` Transfers the Correct Amount in Non-self Transfers
erc20-transfer-correct-amount-self	`transfer` Transfers the Correct Amount in Self Transfers
erc20-transfer-exceed-balance	`transfer` Fails if Requested Amount Exceeds Available Balance
erc20-transfer-false	If `transfer` Returns `false` , the Contract State Is Not Changed
erc20-transfer-never-return-false	`transfer` Never Returns `false`
erc20-transferfrom-revert-from-zero	`transferFrom` Fails for Transfers From the Zero Address

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

Property Name	Title
erc20-allowance-change-state	`allowance` Does Not Change the Contract's State
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

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 TIMEDividend (projects/internet-money-time-dividend/TIMEDividend.sol) In Commit c1c1ea4fa69611185541c2a130ff0dd9e1f90f97

Verification of ERC-20 Compliance

Detailed results for function `transfer`

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

Detailed results for function `totalSupply`

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

Detailed results for function `balanceOf`

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

Detailed results for function `allowance`

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

Detailed results for function `approve`

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

APPENDIX | T.I.M.E. DIVIDEND (TIME) - BNB SMART CHAIN (BSC)

Initial Consultation

General overview of TIME.

(There are three cases to consider: Native to token, token to native, and token to token)

1&2. Swap occurs within in the wallet. A fee of .729% of the USD value of the asset being swapped out of is charged in the form of the native coin for that given chain. Example: $100 of USDC is being swapped to ETH. A fee of $0.729 will be charged. That fee will be paid in the form of ETH.

3&4. Fees are stored in the swap router contract until a user "sweeps" the fees. At which time, the fees are sent to and stored in the TIME contract. Holders of TIME are then credited their portion of fees, which they can claim as frequently as they desire. With no expiration date to claim.

Notes

If an address sells, burns or transfers its tokens, it is still entitled to claim the fees it has been credited in the TIME contract up until the point of sell, burn or transfer. If TIME is burned, new fees coming into the TIME contract will be equitably distributed to remaining TIME holders.

Detailed Notes

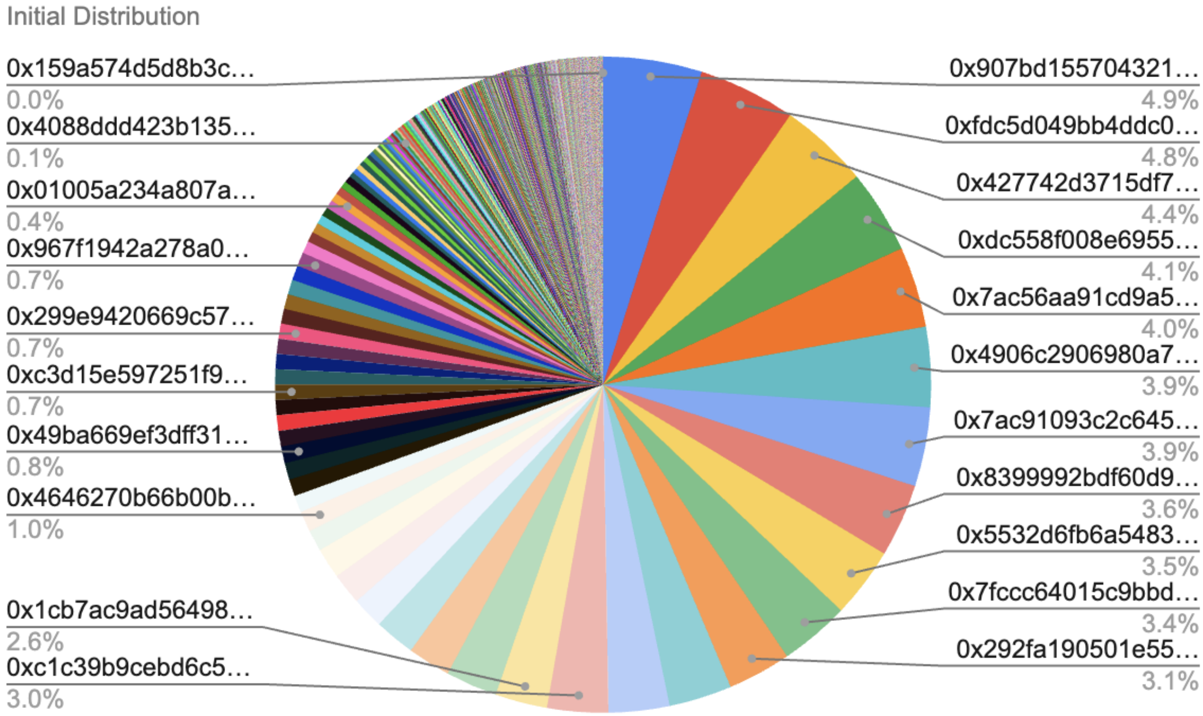
1. While the token has an owner no distribution occurs, only trading of magnified dividend corrections can occur.
2. When funds come into the TIME token contract, they increment a magnified share value which is used to derive a portion of ownership for each address that has a token balance at the time of the distribution. The distribution is additive and non destructive, as in it will provide an equitable share of the income to the contract that holds timedividend and that income will be accessible even if the holder trades away / transfers away their tokens.
3. Ensure there are no ways to extract more value out of the system than is equitable based on ownership during income events.
4. Address should still be able to claim their dividend events that they held after they burn or transfer tokens away. The remaining addresses should not have more or less available to them during the burn, only more after, proportional to their new % ownership of the total supply (% equity).
5. Rounding errors will occur at various points during the calculations - defining these more cleanly + systematically would be helpful.
6. A test is provided in the timedividend.test.ts file that has 3 addresses shifting funds around and burning while income is being distributed. I don't think our pathological cases need to cover less than 2 accounts with balances. A test has been provided that prints out a table that can be seen by running yarn run test:flow. Other pathological cases could include any combination of burning 99.99% percent of the supply, flow of funds being equivalent to the total supply of native token per day (pulsechain ~ 1_200_000x eth) both pulsechain, ethereum, or any other anomalous chains' total supply, perhaps xdai would be a good example.

Initial Distribution

As of Mar 24, 2023, the TIMEDividend contract is deployed to Ethereum Mainnet. The contract address is 0xd08481058399490B83a72676901d4e9dB70E75aC.

We have `0x907bd155704321d8c27d7ce8d9a51452e7eb22b6` to be the address that holds the most tokens. It holds 97178934 TIME, which is around 4.86% of the total distribution.

Below is the pie chart of all token holding addresses. We can see the distribution is sufficiently diverse.



Finding Categories

Categories	Description

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 <
    0x10000000000000000000000000000000000000000 && value >=
    0 && _balances[to] >= 0 && _balances[from] >= 0 && _balances[from] <
    0x10000000000000000000000000000000000000000 &&
    _allowances[from][msg.sender] >= 0 && _allowances[from][msg.sender] <
    0x10000000000000000000000000000000000000000) ==>
  <>(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.

