PolkaFoundry

SMART CONTRACT AUDIT

ZOKYO.

May 6, 2021 | v. 1.0

PASS

Zokyo's Security Team has concluded that this smart contract passes security qualifications to be listed on digital asset exchanges.

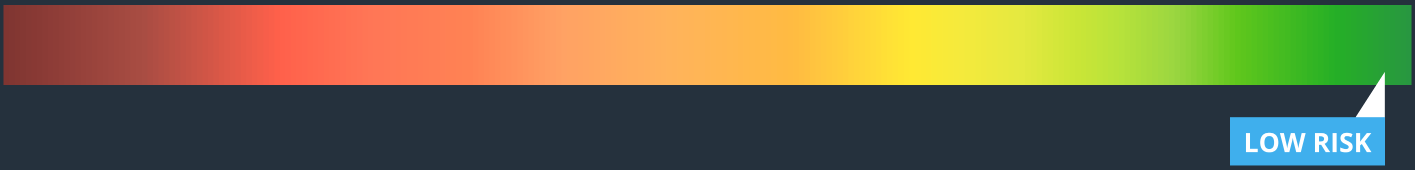
EXCELLENT

TECHNICAL SUMMARY

This document outlines the overall security of the PolkaFoundry smart contracts, evaluated by Zokyo's Blockchain Security team.

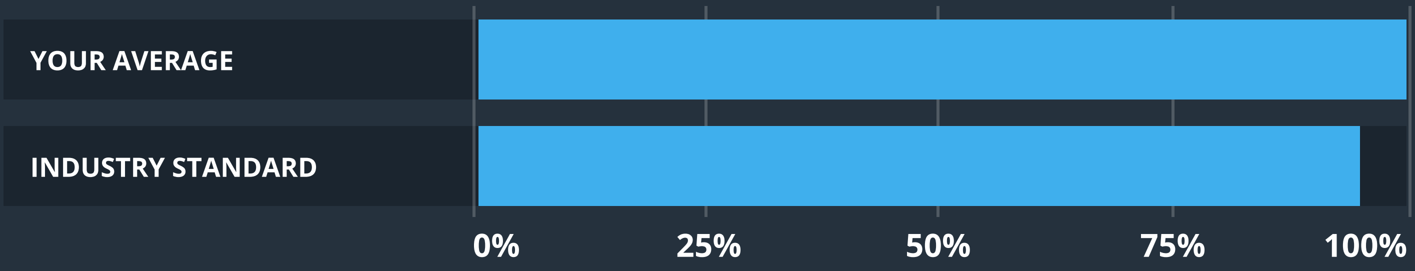
The scope of this audit was to analyze and document the PolkaFoundry smart contract codebase for quality, security, and correctness.

Contract Status



There were no issues found during the audit.

Testable Code



The testable code is 100%, which is above the industry standard of 95%.

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that's able to withstand the Ethereum network's fast-paced and rapidly changing environment, we at Zokyo recommend that the PolkaFoundry team put in place a bug bounty program to encourage further and active analysis of the smart contract.

TABLE OF CONTENTS

AUDITING STRATEGY AND TECHNIQUES APPLIED

The Smart contract's source code was taken from the PolkaFoundry repository – https://github.com/polkafoundry/token/commit/3f8d63079d6a2cdbc65d48547c677dd439eaeec4.
Commit – 3f8d63079d6a2cdbc65d48547c677dd439eaeec4.

Zokyo team has reviewed only PkfToken.sol.

Throughout the review process, care was taken to ensure that the token contract:

- Implements and adheres to existing Token standards appropriately and effectively;
- Documentation and code comments match logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices in efficient use of gas, without unnecessary waste;
- Uses methods safe from reentrance attacks;
- Is not affected by the latest vulnerabilities;
- Whether the code meets best practices in code readability, etc.

Zokyo's Security Team has followed best practices and industry-standard techniques to verify the implementation of PolkaFoundry smart contracts. To do so, the code is reviewed line-by-line by our smart contract developers, documenting any issues as they are discovered. Part of this work includes writing a unit test suite using the Truffle testing framework. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

1 Due diligence in assessing the overall code quality of the codebase.

2 Cross-comparison with other, similar smart contracts by industry leaders.

3 Testing contract logic against common and uncommon attack vectors.

4 Thorough, manual review of the codebase, line-by-line.

EXECUTIVE SUMMARY

There were no issues found during the audit. The contract is well written and structured. Zokyo team is convinced that the contract is fully production-ready.

It is worth mentioning that Zokyo auditors have reviewed just token contract (PkfToken.sol).

STRUCTURE AND ORGANIZATION OF DOCUMENT

For ease of navigation, sections are arranged from most critical to least critical. Issues are tagged “Resolved” or “Unresolved” depending on whether they have been fixed or addressed. Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

● Critical

The issue affects the ability of the contract to compile or operate in a significant way.

● High

The issue affects the ability of the contract to compile or operate in a significant way.

● Medium

The issue affects the ability of the contract to operate in a way that doesn’t significantly hinder its behavior.

● Low

The issue has minimal impact on the contract’s ability to operate.

● Informational

The issue has no impact on the contract’s ability to operate.

COMPLETE ANALYSIS

No issues were identified during the auditing process.

CODE COVERAGE AND TEST RESULTS FOR ALL FILES

Tests written by PolkaFoundry team

```
Contract: PkfToken
    test some simple trades
        ✓ Test data correct after deployed (93ms)
        ✓ Test burn (93ms)
        ✓ Test burnFrom (129ms)


3 passing (811ms)
```

FILE	% STMTS	% BRANCH	% FUNCS	% LINES	UNCOVERED LINES
contracts\	100.00	100.00	100.00	100.00	
PfkToken.sol	100.00	100.00	100.00	100.00	
All files	**100.00**	**100.00**	**100.00**	**100.00**	

Tests written by Zokyo Secured team

As part of our work assisting PolkaFoundry in verifying the correctness of their contract code, our team was responsible for writing integration tests using the Truffle testing framework.

Tests were based on the functionality of the code, as well as a review of the PolkaFoundry contract requirements for details about issuance amounts and how the system handles these.

```
Contract: PkfToken
    contract details
      ✓ should deploy with correct name
      ✓ should deploy with correct symbol
      ✓ should deploy with correct decimals
    initial distribution
      ✓ should deploy with expected total supply
      ✓ should deploy giving expected amount to owner
    burn
      ✓ should be able to burn owned tokens and lower total supply (86ms)
      ✓ should be able to burn allowed tokens and lower total supply (132ms)
     transfer
      ✓ should be able transfer owned tokens (87ms)
      ✓ should be able to transfer allowed tokens (120ms)

9 passing (4s)
```

FILE	% STMTS	% BRANCH	% FUNCS	% LINES	UNCOVERED LINES
contracts\	100.00	100.00	100.00	100.00	
PfkToken.sol	100.00	100.00	100.00	100.00	
All files	**100.00**	**100.00**	**100.00**	**100.00**	

We are grateful to have been given the opportunity to work with the PolkaFoundry team.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them.

Zokyo's Security Team recommends that the PolkaFoundry team put in place a bug bounty program to encourage further analysis of the smart contract by third parties.