Smart Contract Security Audit

Audit details:

Audited project:	Polybear Finance
Deployer address	0xdFDAD394946968e5e7a24B0887d4640C89BbbC48
Blockchain:	Matic
Project website:	https://polybear.exchange

May, 2021
QUANTUM

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and QUANTUM and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (QUANTUM) owe no duty of care towards you or any other person, nor does QUANTUM make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and QUANTUM hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, QUANTUM hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against QUANTUM, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

QUANTUM was commissioned by Polybear Finance to perform an audit of smart contracts:

- Polybear Token: 0xdFDAD394946968e5e7a24B0887d4640C89BbbC48
- MasterChef: 0xC247889548bf7a17a68a0b226e9A75CFbAC17210
- Timelock: 0xB0b6264334b5086fa8ab687172190AeC477B000F

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 16.05.2021.

Contract name:	Polybear Finance
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0xdFDAD394946968e5e7a24B0887d4640C89BbbC48
Total supply:	N/A
Token ticker:	BEAR
Decimals:	18
Contract deployer address:	0xC2e7eD5BEd6464A8dD995B9F9CaF30FC0b9a6924
Fees address:	0x89350FaB13e97d83E22b112b6B3430d26631248d

MasterChef contract details.

Contract name:	MasterChef
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0xC247889548bf7a17a68a0b226e9A75CFbAC17210
Deployer address:	0xC2e7eD5BEd6464A8dD995B9F9CaF30FC0b9a6924
Fee address:	0x89350fab13e97d83e22b112b6b3430d26631248d
Dev address:	0xc2e7ed5bed6464a8dd995b9f9caf30fc0b9a6924
BEAR contract address:	0xdFDAD394946968e5e7a24B0887d4640C89BbbC48
BEAR per block:	5000000000000000000
Contract owner address:	0xb0b6264334b5086fa8ab687172190aec477b000f
Pool length:	35
Start block:	14871175
Total alloc point:	35000

Issues Checking Status

№	Issue description.	Checking status
1	Compiler errors.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Low issues
10	Methods execution permissions.	Passed
11	Economy model of the contract.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Medium issues
19	Cross-function race conditions.	Passed
20	Safe Open Zeppelin contracts implementation and usage.	Passed
21	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

1. Wrong burning

Issue:

There is sending tokens to the dead address in overridden _transfer functions, instead of burning them in the token contract.

Recommendation:

There should be a burn instead of sending to the dead address.

Low Severity Issues

1. Block gas limit

Issue:

The `updateEmissionRate` function can fail due to the block gas limit if the pool size is too big.

2. `add` function issue

Issue:

If some LP token is added to the contract twice using function add, then the total amount of reward in function `updatePool` will be incorrect.

Recommendation:

Add the mapping from address to bool and check that the same address will not be added twice.

Owner privileges

Transfer onwership of BEARToken to Masterchef
https://explorer-mainnet.maticvigil.com/tx/0xae979ab48023b8d29ae55dff6df4e8cc2e1e1acc2b1e16875a130d4b5374abfc/internal-transactions

Transfer ownership of MasterChef to Timelock
https://explorer-mainnet.maticvigil.com/tx/0x15f74925011fded04c8fb1263fa1c0ecac4798d5700363f5c908a2c48d4088ea/internal-transactions

Conclusion

Smart contracts do not contain high severity issues!

QUANTUM note:
Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.