Revoluzion Audit

Audit Report

Name	: PetZ Gold Token
Symbol	: PGT
Decimals	: 18
Address	: 0xb78bf2a671ef8d52a62390772445165507ab7029
Owner	: 0xbc1f556f327da219be7a9e66cde0a1dcbe9a1e65
Network	: Binance Smart Chain (Mainnet)
Type	: BEP20
Audited on	: 1 November 2022
Updated on	: 3 November 2022

Revoluzion Audit

Contents

Project Overview

Name	PetZ Gold Token
Symbol	PGT
Decimals	18
Total Supply	100,000,000 (Initial) 500,000,000 (Capped)
Tax	N/A
Compiler Version	v0.8.0+commit.c7dfd78e
Optimization	Yes with 200 runs
License Type	None
Explorer Link	https://bscscan.com/address/0xb78bf2a671ef8d52a62390772445165507ab7029
Create Tx	0x4587a240c071448a45da804bad8786c6aa752408a1d4a2eafda618428785c478
Creator	0xbc1f556f327da219be7a9e66cde0a1dcbe9a1e65
GitHub Link	https://github.com/petzofficial/petz_contracts
Website	https://petz.money

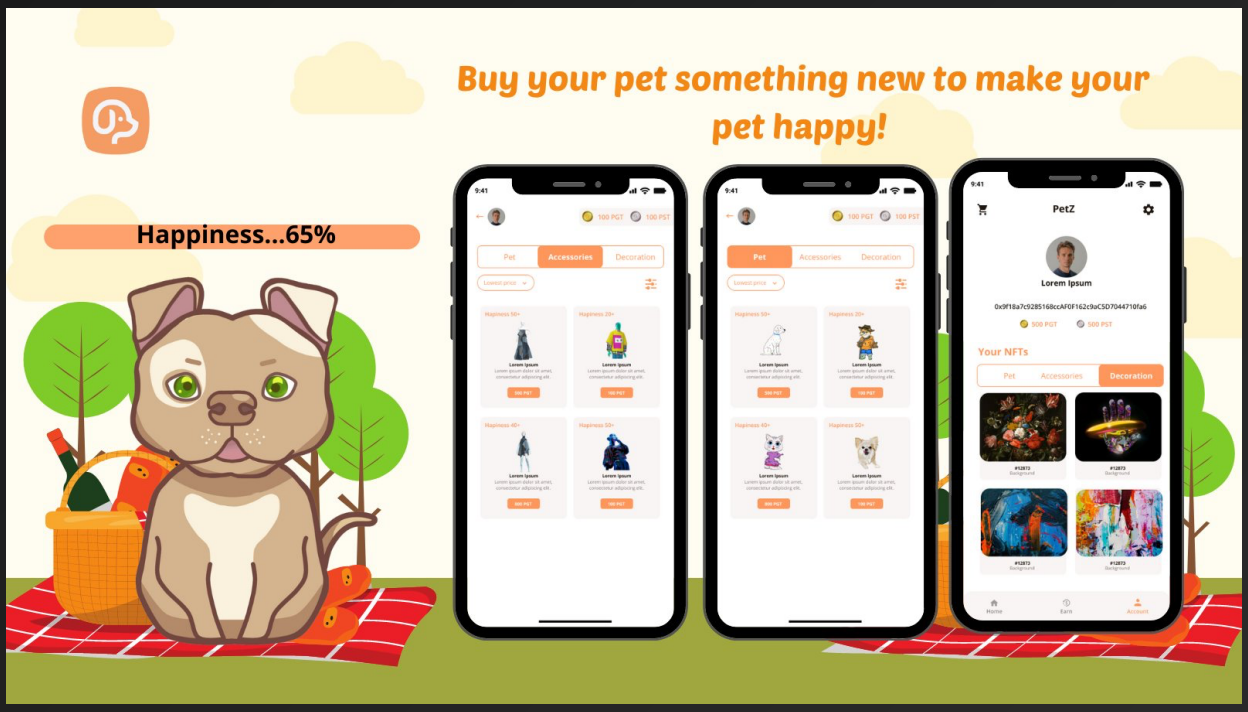
Project Description

According to their website

PetZ Money is a blockchain-powered virtual pet with game-fi elements that reward users based on productivity. User will be able to interact with super cute virtual pets, collect and breed beautiful and exotic animals while exploring the immersive worlds, and customize their avatars. A project that will allow you to own a pet anywhere in the world, as long as you're connected to their petverse.

Release Date : TBA

Category : Governance and utility Token



Online Presence

About Website

Registrar : https://www.sav.com

Domain Expiration : 2023-08-13

SSL Certificate : Issued by Let's Encrypt

Official Links

Website	**https://petz.money**
Twitter	**https://twitter.com/petzofficial**
GitHub	**https://github.com/petzofficial**
Telegram Group	**https://t.me/petz_money**

The Team

About	We only interacted with the owner for the audit. However, there are no KYC procedure being conducted by Revoluzion on any of PetZGoldToken's team members.
KYC Issuer	N/A
Member's KYC'd	N/A
KYC Date	N/A
Certificate Link	N/A
Task Completed	N/A

Audit Overview

Threat Level

When conducting audit on smart contract(s), we first look for known vulnerabilities and issues within the code because any exploitation on such vulnerabilities and issues by malicious actors could potentially result in serious financial damage to the projects. All the issues and vulnerabilities will be categorized into the categories as provided below.

Critical

This category provides issues and vulnerabilities that are critical to the performance/functionality of the smart contract and should be fixed by project creator before moving to a live environment.

Medium

This category provides issues and vulnerabilities that are not that critical to the performance/functionality of the smart contract but is recommended to be fixed by project creator before moving to a live environment.

Minor

This category provides issues and vulnerabilities that are minor to the performance/functionality of the smart contract and can remain unfixed by project creator before moving to a live environment.

Informational

This category provides issues and vulnerability that have insignificant effect on the performance/functionality of the smart contract and can remain unfixed by project creator before moving to a live environment. However, fixing them can further improve the efficacy or security for features with a risk-free factor.

Notable Information

- Contract Owner cannot stop or pause transactions.
- Contract Owner cannot transfer tokens from specific address.
- Contract Owner cannot burn tokens from specific wallet.
- Contract Owner cannot blacklist wallets from selling.
- Contract is using safe Zeppelin modules.
- Contract Owner can no longer mint new tokens after deploying smart contract since the ownership of the smart contract has been transferred to Masterchef contract at 0x4952D8ce9Ffe6f51a2f99bA221620f673bAbC83B.

Caution

- There is one minor compiler warning when compiling the smart contract that should not affect the functionality since it is due to SPDX license identifier not being provided.

Contract Diagnostic

Link for initial smart contract commit being audited on GitHub:

https://github.com/petzofficial/petz_contracts/commit/19f89330ed014c668a60e85afefa7a65312775b6

CODE	SEVERITY	DESCRIPTION
SWC-120	**Minor**	Potential use of "block.number" as source of randomness.
DC	**Informational**	Dead code.
NC	**Informational**	Naming convention.

SWC-120 — Potential use of "block.number" as source of randomness

SEVERITY	Minor
LOCATION(S)	PetZGoldToken.sol#L1167, 1247
DESCRIPTION	The environment variable "block.number" looks like it might be used as a source of randomness to trigger a function.
RECOMMENDATIONS	We would recommend project owner to not use any of the environment variables like coinbase, gaslimit, block number and timestamp as sources of randomness since they are predictable and be aware that such usage could introduces a certain level of trust into miners. Keep in mind that malicious miner can manipulate the value of those variables and that any attackers could also predetermine the hashes of earlier blocks. However, based on our analysis, there's nothing to be done by project owner since in each of the "block.number" value was used as a means to keep track of time/epoch that relates to the trigger of a specific function.
STATUS	**N/A**

DC — Dead code

SEVERITY	Informational — Medium
LOCATION(S)	PetZGoldToken.sol#L99-103, 110-113, 120-128, 135-138, 145, 148, 160-164, 176-179, 191-196, 210-213, 227-230, 245-248, 265-268, 285-288, 382-391, 409-415, 435-437, 445-447, 460-462, 470-477, 485-487, 495-501, 509-511, 519-525, 527-544, 913-928,
DESCRIPTION	[Context._msgData()] (#L76-78) is never used and should be removed. [SafeMath.tryAdd()] (#L99-103) is never used and should be removed. [SafeMath.trySub()] (#L110-113) is never used and should be removed. [SafeMath.tryMul()] (#L120-128) is never used and should be removed. [SafeMath.tryDiv()] (#L135-138) is never used and should be removed. [SafeMath.tryMod()] (#L145-148) is never used and should be removed. [SafeMath.add()] (#L160-164) is never used and should be removed. [SafeMath.sub()] (#L176-179) is never used and should be removed. [SafeMath.mul()] (#L191-196) is never used and should be removed. [SafeMath.div()] (#L210-213) is never used and should be removed. [SafeMath.mod()] (#L227-230) is never used and should be removed. [SafeMath.sub()] (#L245-248) is never used and should be removed.

	[SafeMath.div()] (#L265-268) is never used and should be removed. [SafeMath.mod()] (#L285-288) is never used and should be removed. [Address.isContract()] (#L382-391) is never used and should be removed. [Address.sendValue()] (#L409-415) is never used and should be removed. [Address.functionCall()] (#L435-437) is never used and should be removed. [Address.functionCall()] (#L445-447) is never used and should be removed. [Address.functionCallWithValue()] (#L460-462) is never used and should be removed. [Address.functionCallWithValue()] (#L470-477) is never used and should be removed. [Address.functionStaticCall()] (#L485-487) is never used and should be removed. [Address.functionStaticCall()] (#L495-501) is never used and should be removed. [Address.functionDelegateCall()] (#L509-511) is never used and should be removed. [Address.functionDelegateCall()] (#L519-525) is never used and should be removed. [Address._verifyCallResult()] (#L527-544) is never used and should be removed. [ERC20._burn()] (#L913-928) is never used and should be removed.
RECOMMENDATIONS	Based on our analysis, the ERC20 smart contract is the standard that is a direct fork from Open Zeppelin and were used within the contract itself. Although those functions were never used elsewhere, especially in PetZGoldToken, it's still okay to leave them be.

	It is the same situation for Address and SafeMath smart contracts since they are both a direct fork / reference of the respective library as provided by Open Zepplin. However, for Context smart contract, it is okay for project creator to remove those functions to further optimize the smart contract since they are not used anywhere at all. Doing so will reduce the amount gas required when deploying the smart contract.
STATUS	**N/A**

NC — Naming convention

SEVERITY	Informational — Minor
LOCATION(S)	PetZGoldToken.sol#L189, 1044, 1049
DESCRIPTION	[PetZGoldToken.mint()] (#L1027) parameter "_to" and "_amount" are not in mixedCase. [PetZGoldToken._delegates] (#L1039) variable is not in mixedCase.
RECOMMENDATIONS	For PetZGoldToken smart contract, it is okay for project creator to update the name of the parameters in those functions so that they conform to the standard naming convention.
STATUS	**N/A**

Changelog

3 November 2022 —
https://bscscan.com/tx/0xa2e93c36a34f487a6ce540c760c426468547a544475f1905ffd0c5d03b058fd1

Contract Owner has transferred the ownership of the contract to Masterchef contract at 0x4952D8ce9Ffe6f51a2f99bA221620f673bAbC83B. Project owner can no longer mint new tokens after deploying smart contract. New tokens will only be automatically minted through UpdatePool functions which publicly can be triggered by anyone.

Disclaimer

This report only shows findings based on our limited project analysis according to the good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall online presence and team transparency details of which are set out in this report. To get a full view of our analysis, **it is important for you to read the full report.** Under no circumstances did Revoluzion Audit receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. **Our team provides no guarantees against the sale of team tokens or the removal of liquidity by the project** audited in this document.

While **we have done our best to conduct thorough analysis to produce this report**, it is crucial to note that you should not rely solely on this report and use the content provided in this document as financial advice or a reason to buy any investment. The Our team disclaims any liability against us for the resulting losses based on the you decision made by relying on the content of this report. **You must conduct your own independent investigations before making any decisions** to protect yourselves from being scammed. We go into more detail on this in the disclaimer clause in the next page — please make sure to read it in full.

Full Disclaimer Clause

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 all copies of this report downloaded and/or printed by you. This report is provided for information purposes only, on a non-reliance basis and does not constitute to any investment advice.

No one shall have any right to rely on the report or its contents, and Revoluzion Audit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (collectively known as Revoluzion) owe no duty of care towards you or any other person, nor do we 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 Revoluzion 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, Revoluzion hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Revoluzion, 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, website, social media, and team.