



CFG NINJA AUDITS

Security Assessment

PutinCoin Token

June 13, 2023

Audit Status: Pass





Audit Edition: Advance














POWERED BY
BLADE POOL

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
 Critical	Danger or Potential Problems.
 High	Be Careful or Fail test.
 Low	Pass, Not-Detected or Safe Item.
 Informational	Function Detected

Manual Code Review Risk Results

Contract Priviledge	Description
 Buy Tax	0
 Sale Tax	0
 Cannot Sale	Pass
 Cannot Sale	Pass
 Max Tax	0
 Modify Tax	Not Detected
 Fee Check	Pass
 Is Honeypot?	Not Detected
 Trading Cooldown	Not Detected
 Can Pause Trade?	Owner need to enable trade, so is paused by default.
 Pause Transfer?	Detected, Owner need to enable trading.



Contract Priviledge	Description
● Max Tx?	Pass
● Is Anti Whale?	Not Detected
● Is Anti Bot?	Not Detected
● Is Blacklist?	Not Detected
● Blacklist Check	Pass
● is Whitelist?	Not Detected
● Can Mint?	Pass
● Is Proxy?	Not Detected
● Can Take Ownership?	Not Detected
● Hidden Owner?	Not Detected
● Owner	0x441d67219bd6c133ade11aeb0a5e937103dffed6
● Self Destruct?	Not Detected
● External Call?	Not Detected
● Other?	Not Detected
● Holders	1
● Auditor Confidence	Low

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.



Project Overview

Token Summary

Parameter	Result
Address	0xb67081Fb2AA10cd264725f3BAFa28CD319d40F80
Name	PutinCoin
Token Tracker	PutinCoin (PTC)
Decimals	9
Supply	1,000,000,000
Platform	Ethereum
compiler	v0.8.18+commit.87f61d96
Contract Name	PutinCoin
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/token/0xb67081Fb2AA10cd264725f3BAFa28CD319d40F80#code
Payment Tx	0x1d853112b16b416bca4381b7e99571f3776c356385ef01ab37e0c169674dc079



Main Contract Assessed Contract Name

Name	Contract	Live
PutinCoin	0xb67081Fb2AA10cd264725f3BAFa28CD319d40F80	Yes

TestNet Contract Assessed Contract Name

Name	Contract	Live
PutinCoin	0x1d432cc1e2716F7Eb453B8CcFBf9Fe64A0FF7B9	Yes

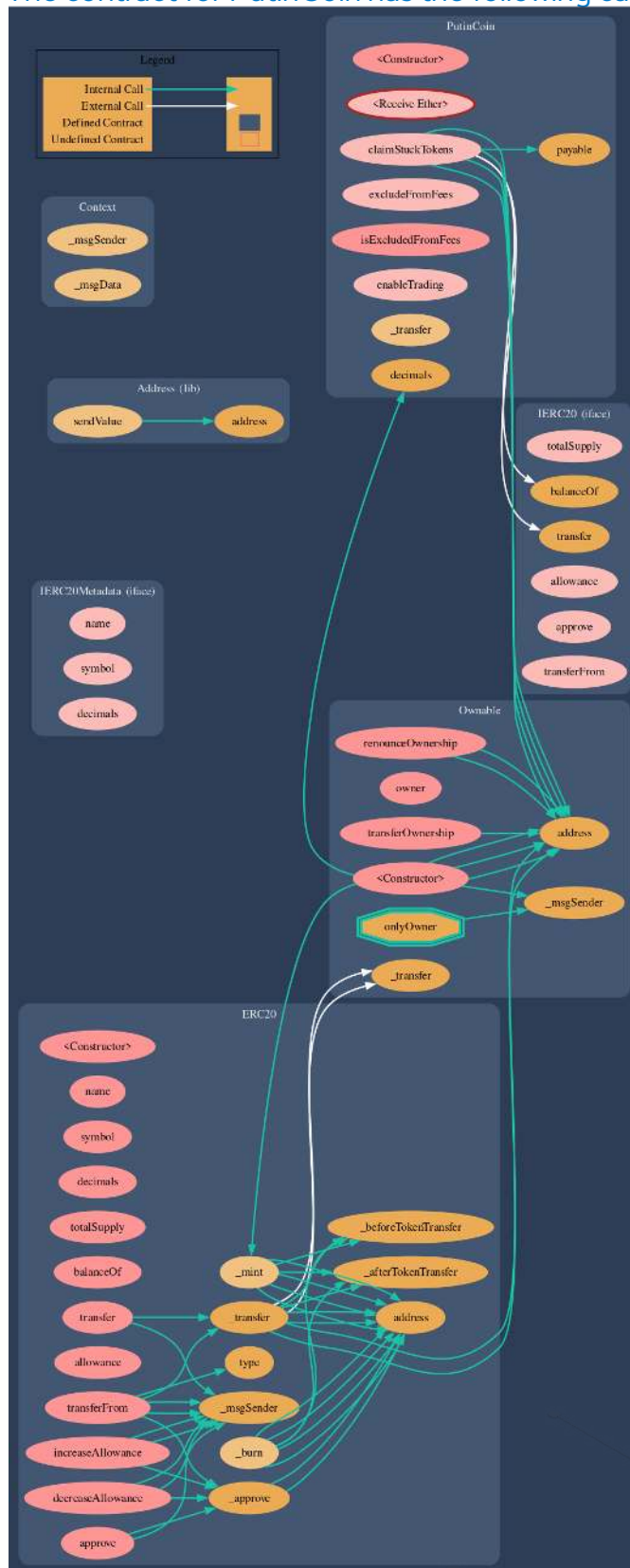
Solidity Code Provided

SolID	File Sha-1	FileName
PutinCoin	2831738143aa9743914b183df22df273fac5d264	putincoin2.sol
PutinCoin		
PutinCoin		
PutinCoin		



Call Graph

The contract for PutinCoin has the following call graph structure.



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	putincoin2.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	putincoin2.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	putincoin2.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	putincoin2.sol	L: 18 C: 5
SWC-104	Medium	Unchecked Call Return Value.	putincoin2.sol	L: 50 C: 24
SWC-105	Pass	Unprotected Ether Withdrawal.	putincoin2.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	putincoin2.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	putincoin2.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	putincoin2.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	putincoin2.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	putincoin2.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	putincoin2.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	putincoin2.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	putincoin2.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	putincoin2.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	putincoin2.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	putincoin2.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	putincoin2.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	putincoin2.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	putincoin2.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	putincoin2.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	putincoin2.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	putincoin2.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	putincoin2.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	putincoin2.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	putincoin2.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	putincoin2.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	putincoin2.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	putincoin2.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	putincoin2.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	putincoin2.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	putincoin2.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	putincoin2.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	putincoin2.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	putincoin2.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	putincoin2.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	putincoin2.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.



Smart Contract Vulnerability Details

SWC-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

References:

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (<https://github.com/ethereum/solidity/releases>) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.



Smart Contract Vulnerability Details

SWC-104 - Unchecked Call Return Value.

CWE-252: Unchecked Return Value.

Description:

The return value of a message call is not checked. Execution will resume even if the called contract throws an exception. If the call fails accidentally or an attacker forces the call to fail, this may cause unexpected behaviour in the subsequent program logic.

Remediation:

If you choose to use low-level call methods, make sure to handle the possibility that the call will fail by checking the return value.

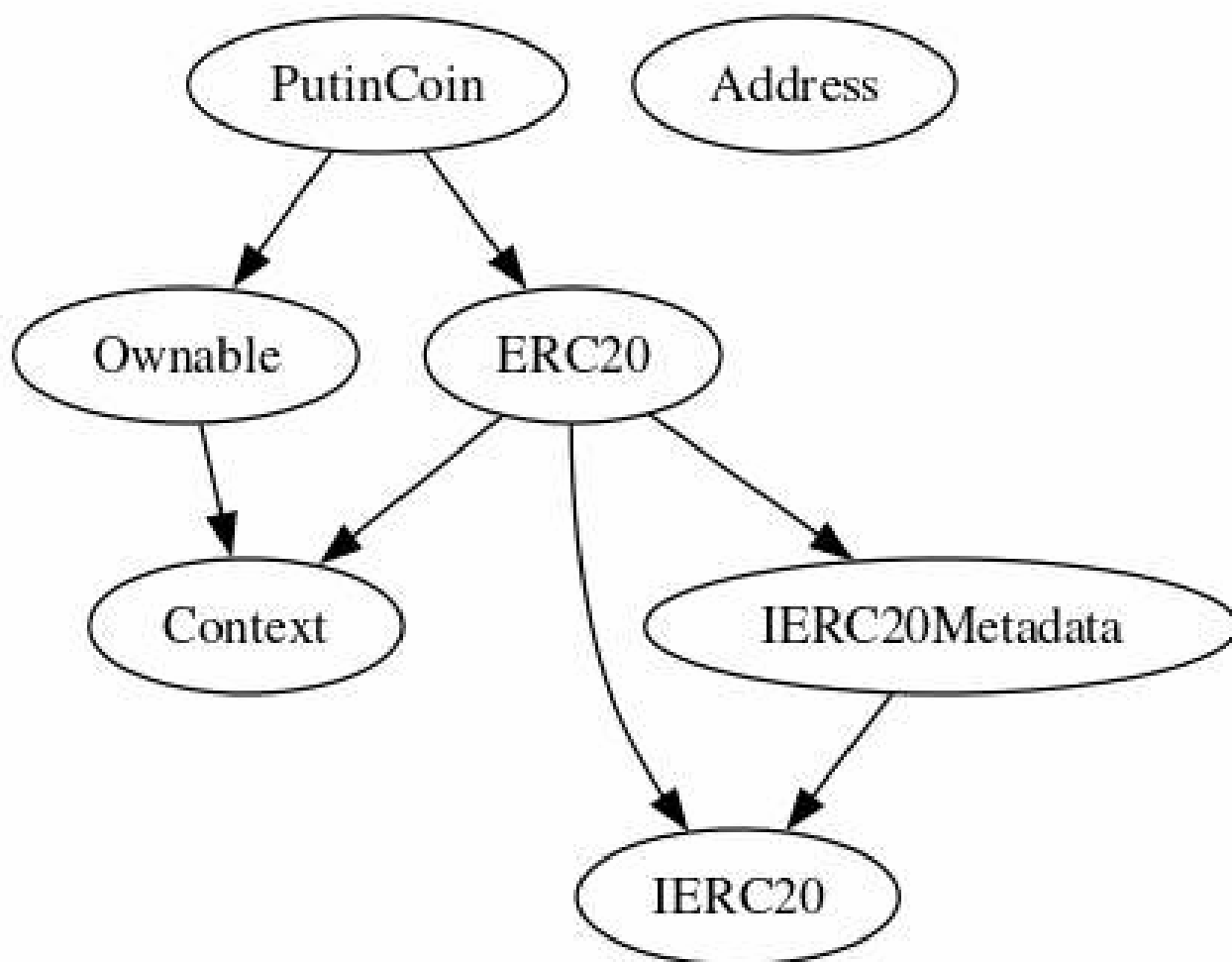
References:

Ethereum Smart Contract Best Practices - Handle errors in external calls.



Inheritance

The contract for PutinCoin has the following inheritance structure.



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
renounceOwnership		Public
transferOwnership	address newOwner	Public
enableTrading		External
excludeFromFees		External
claimStuckTokens		External



Smart Contract Advance Checks



ID	Severity	Name	Result	Status
PTC-01	Minor	Potential Sandwich Attacks.	Pass	Not Detected
PTC-02	Minor	Function Visibility Optimization	Pass	Not Detected
PTC-03	Minor	Lack of Input Validation.	Pass	Not Detected
PTC-04	Major	Centralized Risk In addLiquidity.	Pass	Not Detected
PTC-05	Minor	Missing Event Emission.	Fail	Detected
PTC-06	Minor	Conformance with Solidity Naming Conventions.	Pass	Not Detected
PTC-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
PTC-08	Minor	Dead Code Elimination.	Pass	Not-Found
PTC-09	Major	Third Party Dependencies.	Pass	Not Detected
PTC-10	Major	Initial Token Distribution.	Pass	Not-Found
PTC-11	Minor	AntiBot is present on the transfer.	Pass	Not Detected
PTC-12	Major	Centralization Risks In The X Role	Pass	Not-Found
PTC-13	Informational	Extra Gas Cost For User..	Pass	Not Detected
PTC-14	Medium	Unnecessary Use Of SafeMath	Pass	Detected
PTC-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found



ID	Severity	Name	Result	Status
PTC-16	Medium	Taxes can be up to 100%	Pass	Not-Found
PTC-17	Informational	Conformance to numeric notation best practice.	Pass	Not-Found
PTC-18	Critical	Stop Transactions by using Enable Trade.	Fail	Detected



PTC-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	 Minor	putincoin2.sol: 281, 14	 Detected

Description



Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes. The linked code does not create an event for the transfer.

Remediation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.



PTC-18 | Stop Transactions by using Enable Trade.

Category	Severity	Location	Status
Logical Issue	 Critical	putincoin2.sol: 281, 13	 Detected

Description

Enable Trade is present on the following contract and when combined with Exclude from fees it can be considered a whitelist process, this will allow anyone to trade before others and can represent an issue for the holders.

Remediation






We recommend the project owner to carefully review this function and avoid problems when performing both actions.

Project Action








Technical Findings Summary

Classification of Risk

Severity	Description
 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.
 High	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.
 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
 Low	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.
 Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
 Critical	1	0	0
 High	0	0	0
 Medium	0	0	0
 Low	1	0	0
 Informational	0	0	0
Total	2	0	0



Social Media Checks

Social Media	URL	Result
Twitter		Fail
Other		Fail
Website	http://putincoin.finance	Pass
Telegram		Fail

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:



Assessment Results

Score Results

Review	Score
Overall Score	83/100
Auditor Score	80/100
Review by Section	Score
Manual Scan Score	35/53
SWC Scan Score	33 /37
Advance Check Score	15 /19

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed



Assessment Results

Important Notes:

- No issues or vulnerabilities were found.
- The contract has no tax, the owner needs to enable trading for people to buy and sell, this item was market critical.
- Please DYOR on the project.

Auditor Score =80
Audit Passed



Appendix

Finding Categories

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.

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.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

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 requirements on the input variables than a setter function.

Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all the developers.



Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocacy for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access 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 with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.

