

# Assure DeFi™

The Verification **Gold Standard**™



## Security Assessment **ManaCoin Token**

September 20, 2023

Audit Status: Pass

Audit Edition: Advance Custom



ASSURE DEFI™  
THE VERIFICATION GOLD STANDARD

# 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 Privilege	Description
🟡 Buy Tax	15%
🟡 Sale Tax	20%
🟢 Cannot Sale	Pass
🟢 Cannot Sale	Pass
🟡 Max Tax	20%
🟡 Modify Tax	Yes
🟢 Fee Check	Pass
🟢 Is Honeypot?	Not Detected
🟢 Trading Cooldown	Not Detected
🔴 Can Pause Trade?	Detected, owner need to enable trade.
🔴 Pause Transfer?	Detected, owner need to enable trade.
🟡 Max Tx?	Fail
🟡 Is Anti Whale?	Detected
🟢 Is Anti Bot?	Not Detected

Contract Privilege	Description
● Is Blacklist?	Not Detected
● Blacklist Check	Pass
● is Whitelist?	Detected
● Can Mint?	Pass
● Is Proxy?	Not Detected
● Can Take Ownership?	Not Detected
● Hidden Owner?	Not Detected
● Owner	0xED57c1f805FAE5e0b4Da6D641AbE118D86AEB0e7
● Self Destruct?	Not Detected
● External Call?	Not Detected
● Other?	Not Detected
● Holders	1
● Auditor Confidence	Medium Risk

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	0xA1DB57DEFD15Be659CfBC612A13195adf5b237c6
Name	ManaCoin
Token Tracker	ManaCoin (MNC)
Decimals	18
Supply	100,000,000
Platform	Ethereum
compiler	v0.8.18+commit.87f61d96
Contract Name	ManaCoin
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	<a href="https://etherscan.io/address/0xA1DB57DEFD15Be659CfBC612A13195adf5b237c6#code">https://etherscan.io/address/0xA1DB57DEFD15Be659CfBC612A13195adf5b237c6#code</a>
Payment Tx	Corporate

# Project Overview

## Simulation Summary

Parameter	Result
Transfer From Owner	Pass
Transfer From Holder	Pass
Add Liquidity	Pass
RemoveLiquidity	Pass
Buy from Owner	Pass
Buy from Holder	Pass
Sale from Owner	Pass
Sale from Holder	Pass
Remove Liquidity	Pass
SwapAndLiquify	Pass
SwapAndSale w/Fee	Pass
SwapAndSale TX	<a href="https://testnet.bscscan.com/tx/0x5e296a802ef045e0e441214eebcc99b40ddc4d735ba354ea02bc1025372d3324">https://testnet.bscscan.com/tx/0x5e296a802ef045e0e441214eebcc99b40ddc4d735ba354ea02bc1025372d3324</a>
SwapAndSaleNoFee	Pass
SwapAndSale No/Fee TX	<a href="https://testnet.bscscan.com/tx/0x09a54a3f0bd0b6ae33e94774251769a487d3b627f312655a1824c67b932ad806">https://testnet.bscscan.com/tx/0x09a54a3f0bd0b6ae33e94774251769a487d3b627f312655a1824c67b932ad806</a>
ExcludeFromFees	Pass
LaunchPad	N/A
Pool Creation	N/A

Parameter	Result
Pool Creation TX	
Pool Finalize	N/A
Pool Finalize TX	
Enable	Pass

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.

## **Main Contract Assessed**

### **Contract Name**

Name	Contract	Live
ManaCoin	0xA1DB57DEFD15Be659CfBC612A13195adf5b237c6	Yes

## **TestNet Contract Assessed**

### **Contract Name**

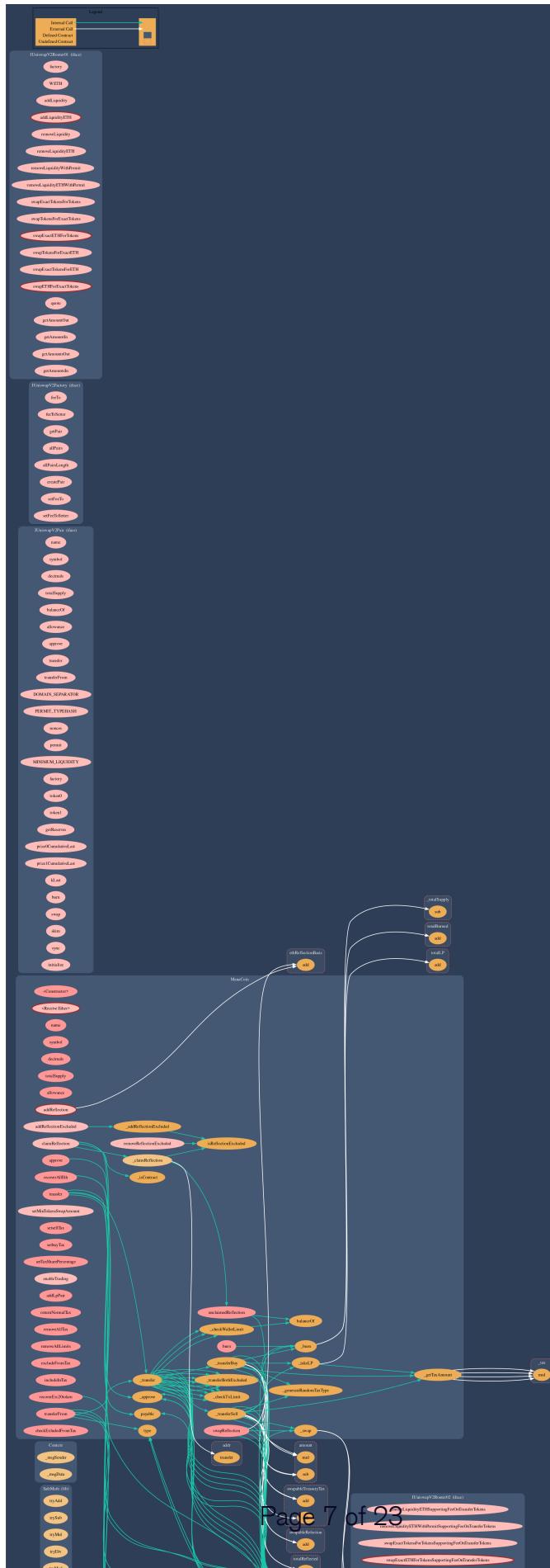
Name	Contract	Live
ManaCoin	00xd8383c3508f79812636222603758Fe99b8aeDf14	Yes

## **Solidity Code Provided**

SolidID	File Sha-1	FileName
MNC	84b61d0691d1bde525d493f7e6b2a14f1d4351b5	manacoin.sol
MNC		
MNC		
MNC		

# Call Graph

The contract for ManaCoin 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	manacoin.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	manacoin.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	manacoin.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	manacoin.sol	L: 14 C: 0
SWC-104	Pass	Unchecked Call Return Value.	manacoin.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	manacoin.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	manacoin.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	manacoin.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	manacoin.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	manacoin.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	manacoin.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	manacoin.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	manacoin.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	manacoin.sol	L: 0 C: 0

<b>ID</b>	<b>Severity</b>	<b>Name</b>	<b>File</b>	<b>location</b>
SWC-114	Pass	Transaction Order Dependence.	manacoin.sol	L: 0 C: 0
SWC-115	Low	Authorization through tx.origin.	manacoin.sol	L: 770 C: 102
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	manacoin.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	manacoin.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	manacoin.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	manacoin.sol	L: 0 C: 0
SWC-120	Low	Potential use of block.number as source of randomness.	manacoin.sol	L: 770 C: 113
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	manacoin.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	manacoin.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	manacoin.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	manacoin.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	manacoin.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	manacoin.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	manacoin.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	manacoin.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	manacoin.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	manacoin.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	manacoin.sol	L: 0 C: 0

<b>ID</b>	<b>Severity</b>	<b>Name</b>	<b>File</b>	<b>location</b>
SWC-132	Pass	Unexpected Ether balance.	manacoin.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	manacoin.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	manacoin.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	manacoin.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	manacoin.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-115 - Authorization through tx.origin

### CWE-477: Use of Obsolete Function

#### Description:

tx.origin is a global variable in Solidity which returns the address of the account that sent the transaction. Using the variable for authorization could make a contract vulnerable if an authorized account calls into a malicious contract. A call could be made to the vulnerable contract that passes the authorization check since tx.origin returns the original sender of the transaction which in this case is the authorized account.

#### Remediation:

tx.origin should not be used for authorization. Use msg.sender instead.

#### References:

Solidity Documentation - tx.origin

Ethereum Smart Contract Best Practices - Avoid using tx.origin

SigmaPrime - Visibility.

# **Smart Contract Vulnerability Details**

## **SWC-120 - Weak Sources of Randomness from Chain Attributes**

### **CWE-330: Use of Insufficiently Random Values**

#### **Description:**

Solidity allows for ambiguous naming of state variables when inheritance is used. Contract A with a variable x could inherit contract B that also has a state variable x defined. This would result in two separate versions of x, one of them being accessed from contract A and the other one from contract B. In more complex contract systems this condition could go unnoticed and subsequently lead to security issues.

Shadowing state variables can also occur within a single contract when there are multiple definitions on the contract and function level.

#### **Remediation:**

Using commitment scheme, e.g. RANDAO. Using external sources of randomness via oracles, e.g. Oraclize. Note that this approach requires trusting in oracle, thus it may be reasonable to use multiple oracles. Using Bitcoin block hashes, as they are more expensive to mine.

#### **References:**

How can I securely generate a random number in my smart contract?)

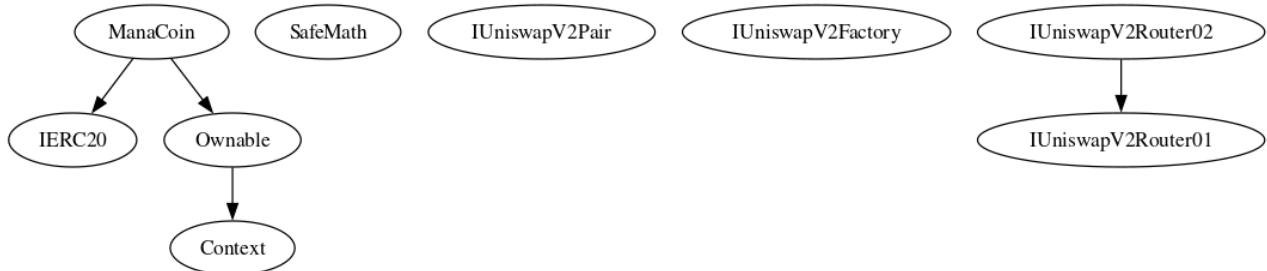
When can BLOCKHASH be safely used for a random number? When would it be unsafe?

The Run smart contract.

# Inheritance

**The contract for ManaCoin has the following inheritance structure.**

**The Project has a Total Supply of 100,000,000**



# Smart Contract Advance Checks

ID	Severity	Name	Result	Status
MNC-01	Low	Potential Sandwich Attacks.	Pass	Not Detected
MNC-02	Informational	Function Visibility Optimization	Pass	Resolved
MNC-03	Low	Lack of Input Validation.	Fail	Detected
MNC-04	High	Centralized Risk In addLiquidity.	Pass	Not Detected
MNC-05	Low	Missing Event Emission.	Fail	Detected
MNC-06	Low	Conformance with Solidity Naming Conventions.	Pass	Not Detected
MNC-07	Low	State Variables could be Declared Constant.	Pass	Not Detected
MNC-08	Low	Dead Code Elimination.	Pass	Not Detected
MNC-09	High	Third Party Dependencies.	Pass	Not Detected
MNC-10	High	Initial Token Distribution.	Pass	Not Detected
MNC-11	Medium	'difficulty' was replaced by 'prevrandaو'	Pass	Resolved
MNC-12	High	Centralization Risks In The X Role	Pass	Not Detected
MNC-13	Informational	Extra Gas Cost For User..	Pass	Not Detected
MNC-14	Medium	Unnecessary Use Of SafeMath	Pass	Resolved
MNC-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not Detected
MNC-16	Medium	Taxes can be up to 100%	Pass	Not Detected
MNC-17	Logical Issue	Conformance to numeric notation best practice.	Pass	Not Detected
MNC-18	Critical	Stop Transactions by using Enable Trade.	Fail	Detected

## MNC-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	 Low	manacoin.sol: L: 717 C: 14,L: 726 C: 12	 Detected

### Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the .

### Remediation

We advise the client to add the check for the passed-in values to prevent unexpected errors as below:

```
...
require(receiver != address(0), "Receiver is the zero address");
...
...
require(value X limitation, "Your not able to do this function");
...
```

We also recommend customer to review the following function that is missing a required validation. .

## MNC-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	 Low	manacoin.sol: L: 717 C: 14,L: 726 C: 12	 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.

## MNC-18 | Stop Transactions by using Enable Trade.

Category	Severity	Location	Status
Logical Issue	<span style="color: red;">●</span> Critical	manacoin.sol: L: 722 C: 0	<span style="color: blue;">■</span> 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 and 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
<span style="color: red;">●</span> 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.
<span style="color: orange;">●</span> 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.
<span style="color: yellow;">●</span> Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
<span style="color: green;">◆</span> 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.
<span style="color: blue;">ℹ</span> 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
<span style="color: red;">●</span> Critical	1	0	0
<span style="color: orange;">●</span> High	0	0	0
<span style="color: yellow;">●</span> Medium	0	0	2
<span style="color: green;">◆</span> Low	2	0	0
<span style="color: blue;">ℹ</span> Informational	0	0	1
Total	3	0	3

# Social Media Checks

Social Media	URL	Result
Twitter	<a href="https://twitter.com/ManaCoinETH">https://twitter.com/ManaCoinETH</a>	Pass
Other	<a href="https://medium.com/@ManaCoinETH">https://medium.com/@ManaCoinETH</a>	Pass
Website	<a href="https://www.manacoin.io/">https://www.manacoin.io/</a>	Pass
Telegram	<a href="https://t.me/ManaCoinETH">https://t.me/ManaCoinETH</a>	Pass

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	81/100
Auditor Score	80/100
Review by Section	Score
Manual Scan Score	18/53
SWC Scan Score	33 /37
Advance Check Score	30 /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:**

- Initial Buy Tax is 15% and initial sale tax is 20%, the owner can then set then to 6% via a function or via a function called returnNormalTax that is 5%.
- There are a few items from a code perspective that need to be re-evaluated.
- The owner needs to enable trade.
- dxRouter is not excluded from Fees, so removing liquidity incurs in fees, even while the msg.sender is the owner.

**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 require statements 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

Assure Defi 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 depreciation 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 Assure Defi is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will Assure Defi 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 Assure Defi 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.

