MANATY

Technical Audit Company

Klubcoin Token
Smart Contract Security Audit

Performed by: Sebastien Michea

On: February 12, 2022

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. 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 based on 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 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 Manaty and its affiliates (including holding companies, shareholders, subsidiaries, employees, providers, directors, officers, and other representatives) (**Manaty**) owe no duty of care towards you or any other person, nor does **Manaty** 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 Manaty 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, **Manaty** hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against **Manaty**, 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.

Context

Manaty was commissioned by The Klub SAS to perform an audit of the smart contract :

https://etherscan.io/address/0xf993c2749a21d10a4a36fe5dda23830b415d9e0d#code

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.

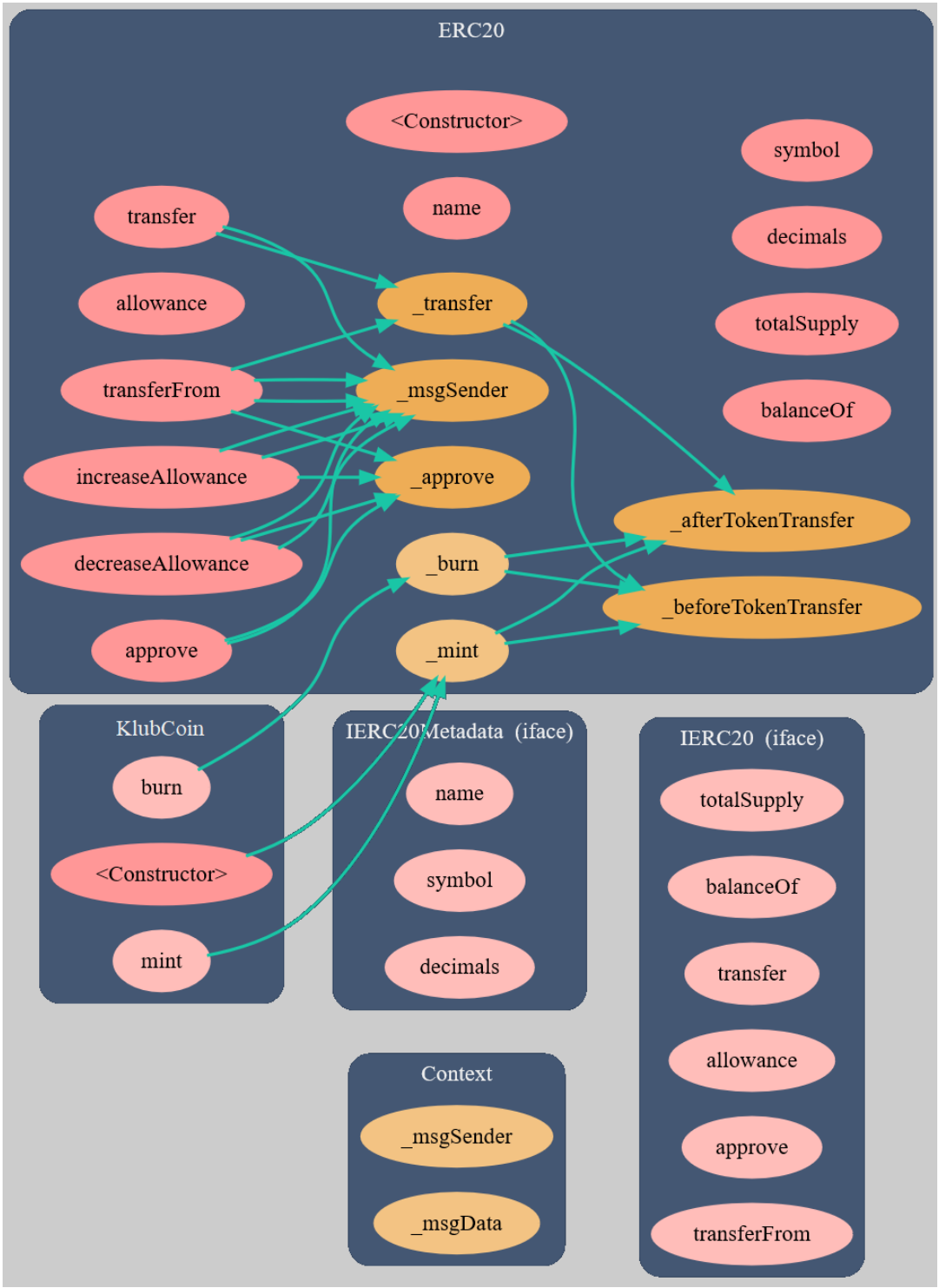
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

The analysis of the security is purely based on the smart contract alone. No application, operation or product code were reviewed for security.

Contracts Details

Contract name	KlubCoin
Contract address	0xf993c2749A21d10a4a36Fe5ddA23830b415D9E0D
Total supply	1,000,000,000
Token ticker	KLUB
Decimals	18
Token holders	1
Transactions count	1
Top 100 holders dominance	100.00%
Launched at	Feb-06-2022 09:17:05 PM +UTC
Contract deployer address	0x3fd49b634900d00b0160bf574fa71bf863513449
Contract's current owner address	0x3fd49b634900d00b0160bf574fa71bf863513449

Contract Method Flow Diagram



Contract functions details

Contract	Type	Bases		
└	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
IERC20Interface	Interface			
└	totalSupply	External ❗		NO ❗
└	balanceOf	External ❗		NO ❗
└	transfer	External ❗	🛑	NO ❗
└	allowance	External ❗		NO ❗
└	approve	External ❗	🛑	NO ❗
└	transferFrom	External ❗	🛑	NO ❗
IERC20Metadata	Interface	IERC20		
└	name	External ❗		NO ❗
└	symbol	External ❗		NO ❗
└	decimals	External ❗		NO ❗
ERC20	Implementation	Context, IERC20, IERC20Metadata		
└	<Constructor>	Public ❗	🛑	NO ❗
└	name	Public ❗		NO ❗
└	symbol	Public ❗		NO ❗
└	decimals	Public ❗		NO ❗
└	totalSupply	Public ❗		NO ❗
└	balanceOf	Public ❗		NO ❗
└	transfer	Public ❗	🛑	NO ❗
└	allowance	Public ❗		NO ❗
└	approve	Public ❗	🛑	NO ❗
└	transferFrom	Public ❗	🛑	NO ❗
└	increaseAllowance	Public ❗	🛑	NO ❗
└	decreaseAllowance	Public ❗	🛑	NO ❗
└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
└	_beforeTokenTransfer	Internal 🔒	🛑	
Klubcoin	Implementation	ERC20		
└	<Constructor>	Public ❗	🛑	ERC20
└	mint	External ❗	🛑	NO ❗
└	burn	External ❗	🛑	NO ❗

Symbol Meaning

🛑 Function can modify state

Issues Checking Satus

	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.	Passed
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.	Passed
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 Issue was found

☑ Medium Severity Issues
No medium severity issue found

☑ Low Severity Issues
No low severity issues found.

Other remarks

The contract owner can mint any amount on any address.

The contract owner can burn any amount of his own coins.

From Solidity ^0.6.8 SPDX license is introduced: https://forum.openzeppelin.com/t/solidity-0-6-8-introduces-spdx-license-identifiers/2859

A SPDX-License-Identifier should be present in the code.
For example the smart contract could use license identifier like

```
// SPDX-License-Identifier: MIT
```

Conclusion

The Smart contract does not contain high severity issues!

Manaty 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.

https://www.credential.net/675606e3-333c-4dd9-b0f7-4300dba340f3#gs.pfqh7r

https://www.credential.net/c590c184-1b67-4de7-9c40-1dec2a2823a5#gs.ledx5t