RugFreeCoins Audit

POOH Token
Smart Contract Security Audit

May 06th ,2023

Contents

Audit details

Audited project
POOH Token

Contract Address
0xb69753c06bb5c366be51e73bfc0cc2e3dc07e371

Client contact
POOH Token Team

Blockchain
Ethereum smart chain

Project website
https://pooh.money/

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

Overview

✅ No mint function found, the owner cannot mint tokens after initial deployment.

✅ The owner can’t set a max transaction limit

✅ The owner can’t pause trading.

✅ The owner can't set fees over 25%.

✅ The owner can't blacklist wallets.

✅ The owner can’t set a max wallet limit

✅ The owner can’t claim the contract’s balance of its own token.

Background

Rugfreecoins was commissioned by the POOH Token Team to perform an audit of the smart contract.

https://etherscan.io/token/0xb69753c06bb5c366be51e73bfc0cc2e3dc07e371

The focus of this audit is to verify that the smart contract is secure, resilient, and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, and long-term sustainability, and as a guide to improving the smart contract's security posture by remediating the identified issues.

.

Roadmap

Launch & Promotion

- Launch POOH on Uniswap and other popular decentralized exchanges.
- Announce POOH on social media channels like Twitter and Discord and crypto forums like Bitcoin Talk and Reddit
- Early adopters are incentivized and rewarded for being early and then helping spread the word.
- Approach influencers and crypto publications to promote and build awareness of POOH.
- List on popular price tracking websites like Coinmarketcap and CoinGecko.

Community building & expansion

- Engage with the POOH community through social media channels
- Advocate for others to start their own POOH-focused community
- Recommend top mobile apps and web wallets support POOH for easy access
- Expand the use cases of POOH through partnerships with merchants or integration with other DeFi projects

Long-term sustainability & growth

- Continuously expand POOH availability to incentivize holding and reduce volatility
- Diversify supporting teams and allocate resources toward further development and marketing efforts
- Explore new opportunities for growth, such as launching additional exchanges or integrating with other blockchain networks
- Foster a strong and dedicated community to ensure the long-term sustainability and growth of POOH

Tokenomics

0% when buying & selling

Target market and the concept

Target market

- Anyone who's interested in the Crypto space with long-term investment plans.
- Anyone who's ready to earn a passive income by holding tokens.
- Anyone who's interested in trading tokens.
- Anyone who's interested in taking part in the POOH ecosystem.
- Anyone who's interested in taking part in the future plans of POOH Token.
- Anyone who's interested in making financial transactions with any other party using POOH Token as the currency.

Potential to grow with score points

1.	Project efficiency	9/10
2.	Project uniqueness	9/10
3	Information quality	9/10
4	Service quality	9/10
5	System quality	9/10
6	Impact on the community	10/10
7	Impact on the business	10/10
8	Preparing for the future	10/10
9	Smart contract security	10/10
10	Smart contract functionality assessment	10/10
Total Points		**9.5/10**

Contract details

Token contract details for 6th of May 2023

Contract name	POOH
Contract address	0xB69753c06BB5c366BE51E73bFc0cC2e3DC07E371
Token supply	420,690,000,000,000
Token ticker	POOH
Decimals	18
Token holders	6,124
Transaction count	27,489
Contract deployer address	0x5e58c97F781f98d70F9b72e69629312bF70EBaf4
Contract's current owner address	0x0000000000000000000000000000000000000000

Contract code function details

No	Category	Item	Result
1	Coding conventions	BRC20 Token standards	pass
		compile errors	pass
		Compiler version security	pass
		visibility specifiers	pass
		Gas consumption	pass
		SafeMath features	pass
		Fallback usage	pass
		tx.origin usage	pass
		deprecated items	pass
		Redundant code	pass
		Overriding variables	pass
2	Function call audit	Authorization of function call	pass
		Low level function (call/delegate call) security	pass
		Returned value security	pass
		Selfdestruct function security	pass
3	Business security	Access control of owners	
		Business logics	pass
		Business implementations	pass
4	Integer overflow/underflow		pass
5	Reentrancy		pass
6	Exceptional reachable state		pass
7	Transaction ordering dependence		pass
8	Block properties dependence		pass
9	Pseudo random number generator (PRNG)		pass
10	DoS (Denial of Service)		pass
11	Token vesting implementation		pass
12	Fake deposit		pass

13	**Event security**		**pass**

Contract description table

The below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions, and implementations with their visibility and mutability.

Contract	**Type**	**Bases**		
L	Function Name	Visibility	Mutability	Modifiers
POOH	**Implementation**	**ERC20, ERC20 Burnable, ERC20Permit, ERC20Votes, Ownable**		
L		Public !	🛑	ERC20 ERC20Permit
L	_afterTokenTransfer	Internal 🔒	🛑	
L	_mint	Internal 🔒	🛑	
L	_burn	Internal 🔒	🛑	
ERC20	**Implementation**	**Context, IERC20, IERC20 Metadata**		
L		Public !	🛑	NO !
L	name	Public !		NO !
L	symbol	Public !		NO !
L	decimals	Public !		NO !
L	totalSupply	Public !		NO !
L	balanceOf	Public !		NO !

L	transfer	Public !	🛑	NO !
L	allowance	Public !		NO !
L	approve	Public !	🛑	NO !
L	transferFrom	Public !	🛑	NO !
L	increaseAllowance	Public !	🛑	NO !
L	decreaseAllowance	Public !	🛑	NO !
L	_transfer	Internal 🔒	🛑	
L	_mint	Internal 🔒	🛑	
L	_burn	Internal 🔒	🛑	
L	_approve	Internal 🔒	🛑	
L	_spendAllowance	Internal 🔒	🛑	
L	_beforeTokenTransfer	Internal 🔒	🛑	
L	_afterTokenTransfer	Internal 🔒	🛑	
IERC20	**Interface**			
L	totalSupply	External !		NO !
L	balanceOf	External !		NO !
L	transfer	External !	🛑	NO !
L	allowance	External !		NO !
L	approve	External !	🛑	NO !
L	transferFrom	External !	🛑	NO !

IERC20 Metadata	**Interface**	**IERC20**		
└	name	External !		NO !
└	symbol	External !		NO !
└	decimals	External !		NO !
Context	**Implementation**			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
ERC20 Burnable	**Implementation**	**Context, ERC20**		
└	burn	Public !	🛑	NO !
└	burnFrom	Public !	🛑	NO !
ERC20Permit	**Implementation**	**ERC20, IERC20Permit, EIP712**		
└		Public !	🛑	EIP712
└	permit	Public !	🛑	NO !
└	nonces	Public !		NO !
└	DOMAIN_SEPARATOR	External !		NO !
└	_useNonce	Internal 🔒	🛑	
IERC20 Permit	**Interface**			

└	permit	External !		NO !
└	nonces	External !		NO !
└	DOMAIN_SEPARATOR	External !		NO !
ECDSA	**Library**			
└	_throwError	Private		
└	tryRecover	Internal		
└	recover	Internal		
└	tryRecover	Internal		
└	recover	Internal		
└	tryRecover	Internal		
└	recover	Internal		
└	toEthSignedMessageHash	Internal		
└	toEthSignedMessageHash	Internal		
└	toTypedDataHash	Internal		
Strings	**Library**			
└	toString	Internal		
└	toHexString	Internal		
└	toHexString	Internal		
└	toHexString	Internal		

Math	Library			
L	max	Internal 🔒		
L	min	Internal 🔒		
L	average	Internal 🔒		
L	ceilDiv	Internal 🔒		
L	mulDiv	Internal 🔒		
L	mulDiv	Internal 🔒		
L	sqrt	Internal 🔒		
L	sqrt	Internal 🔒		
L	log2	Internal 🔒		
L	log2	Internal 🔒		
L	log10	Internal 🔒		
L	log10	Internal 🔒		
L	log256	Internal 🔒		
L	log256	Internal 🔒		
EIP712	**Implementation**			
L		Public ❗	🛑	NO ❗
L	_domainSeparatorV4	Internal 🔒		
L	_buildDomainSeparator	Private 🔐		
L	_hashTypedDataV4	Internal 🔒		

Counters	Library			
L	current	Internal 🔒		
L	increment	Internal 🔒	🛑	
L	decrement	Internal 🔒	🛑	
L	reset	Internal 🔒	🛑	
ERC20Votes	**Implementation**	**IVotes, ERC20Permit**		
L	checkpoints	Public ❗		NO ❗
L	numCheckpoints	Public ❗		NO ❗
L	delegates	Public ❗		NO ❗
L	getVotes	Public ❗		NO ❗
L	getPastVotes	Public ❗		NO ❗
L	getPastTotalSupply	Public ❗		NO ❗
L	_checkpointsLookup	Private 🔐		
L	delegate	Public ❗	🛑	NO ❗
L	delegateBySig	Public ❗	🛑	NO ❗
L	_maxSupply	Internal 🔒		
L	_mint	Internal 🔒	🛑	
L	_burn	Internal 🔒	🛑	
L	_afterTokenTransfer	Internal 🔒	🛑	
L	_delegate	Internal 🔒	🛑	

└	_moveVotingPower	Private		
└	_writeCheckpoint	Private		
└	_add	Private		
└	_subtract	Private		
└	_unsafeAccess	Private		
IVotes	**Interface**			
└	getVotes	External !		NO !
└	getPastVotes	External !		NO !
└	getPastTotalSupply	External !		NO !
└	delegates	External !		NO !
└	delegate	External !		NO !
└	delegateBySig	External !		NO !
SafeCast	**Library**			
└	toUint248	Internal		
└	toUint240	Internal		
└	toUint232	Internal		
└	toUint224	Internal		
└	toUint216	Internal		
└	toUint208	Internal		
└	toUint200	Internal		

L	toUint192	Internal		
L	toUint184	Internal		
L	toUint176	Internal		
L	toUint168	Internal		
L	toUint160	Internal		
L	toUint152	Internal		
L	toUint144	Internal		
L	toUint136	Internal		
L	toUint128	Internal		
L	toUint120	Internal		
L	toUint112	Internal		
L	toUint104	Internal		
L	toUint96	Internal		
L	toUint88	Internal		
L	toUint80	Internal		
L	toUint72	Internal		
L	toUint64	Internal		
L	toUint56	Internal		
L	toUint48	Internal		
L	toUint40	Internal		
L	toUint32	Internal		

L	toUint24	Internal		
L	toUint16	Internal		
L	toUint8	Internal		
L	toUint256	Internal		
L	toInt248	Internal		
L	toInt240	Internal		
L	toInt232	Internal		
L	toInt224	Internal		
L	toInt216	Internal		
L	toInt208	Internal		
L	toInt200	Internal		
L	toInt192	Internal		
L	toInt184	Internal		
L	toInt176	Internal		
L	toInt168	Internal		
L	toInt160	Internal		
L	toInt152	Internal		
L	toInt144	Internal		
L	toInt136	Internal		
L	toInt128	Internal		
L	toInt120	Internal		

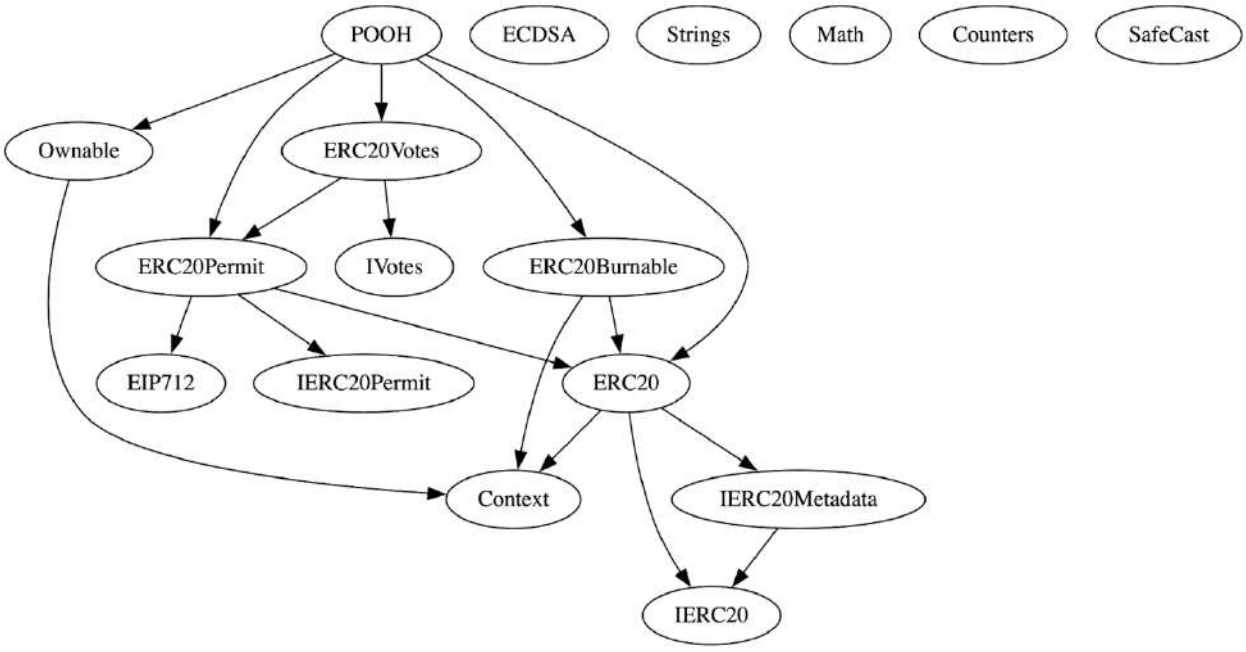
L	toInt112	Internal 🔒		
L	toInt104	Internal 🔒		
L	toInt96	Internal 🔒		
L	toInt88	Internal 🔒		
L	toInt80	Internal 🔒		
L	toInt72	Internal 🔒		
L	toInt64	Internal 🔒		
L	toInt56	Internal 🔒		
L	toInt48	Internal 🔒		
L	toInt40	Internal 🔒		
L	toInt32	Internal 🔒		
L	toInt24	Internal 🔒		
L	toInt16	Internal 🔒		
L	toInt8	Internal 🔒		
L	toInt256	Internal 🔒		
Ownable	**Implementation**	**Context**		
L		Public ❗	🛑	NO ❗
L	owner	Public ❗		NO ❗
L	_checkOwner	Internal 🔒		
L	renounceOwnership	Public ❗	🛑	onlyOwner

L	transferOwnership	Public !	🛑	onlyOwner
L	_transferOwnership	Internal 🔒	🛑	

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Inheritance Hierarchy



Security issue checking status

- **High severity issues**
  No High severity issues found

- **Medium severity issues**
  No medium severity issues found

- **Low severity issues**
  No low-severity issues found

- **Centralization Risk**
  No centralization issues found

Owner privileges

No ownership functions and ownership has been renounced.

Audit conclusion

RugFreeCoins team has performed in-depth testings, line-by-line manual code review, and automated audit of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, manipulations, and hacks. According to the smart contract audit.

Smart contract functional Status: **PASS**

Number of risk issues: **0**

Solidity code functional issue level: **PASS**

Number of owner privileges: **0**

Centralization risk correlated to the active owner: **NONE**

Smart contract active ownership: **NO**