



SMART CONTRACT SECURITY AUDIT

WATCHTOWER

AUDIT DETAILS



Project Name

Daddy Shark



Contract address

0x317D7512f9B73d5907E1a3731AefD5c40353E662



Deployer Address:

0x9ae63330342d1696ec71055df3dd4daab5cd848a



Blockchain

Binance Smart Chain



Project website:

<https://www.babysharktoken.com>



DISCLAIMER

Watchtower has completed this report to provide a summary of the Smart Contract functions, and any security, dependency or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as at the date of this report. In order to understand the full scope of our analysis, it is vital for you to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against Watchtower or its Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your own independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

DISCLAIMER: By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any and all duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise, and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and Watchtower and its members (including holding companies, shareholders, backups, representatives, chiefs, officers and other agents) Watchtower and its subsidiaries owe no obligation of care towards you or any other person, nor does Watchtower make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:

Watchtower is an Anti-Scam Token Utility which reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity.

Watchtowers Development Team consists of a number of Smart Contract creators, Auditors Developers and Blockchain experts.

Watchtowers Website Scanner reviews a number of Risk factors to provide an adequate Risk summary of token projects.

In Addition to this the team also helps with Creation of Smart Contracts for legitimate projects, Audits and Promotion.





OVERVIEW

Watchtower was contracted by Daddy Shark to complete a Smart Contract audit
The objective of the Audit is to achieve the following:

- Provide an Overview and Summary of the Token project.
- Review Team competency and identify risks
- Ensure that the Smart Contract functions are necessary and operate as intended.
- Identify any vulnerabilities in the Smart Contract code.

DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please do invest at your own risk.

(<https://www.cryptowatchtower.io/>)



SMART CONTRACT REVIEW



Contract Created on 08.02.2021

Contract name	Daddy Shark
Contract address	0x317D7512f9B73d5907E1a3731AefD5c40353E662
Total supply	1,000,000,000,000,000
Token ticker	DaddyShark
Decimals	9
Token holders	1
Transactions count	1
Top 100 holders dominance	100.00%
Tax fee	14-16%
Total fees	0
Contract deployer address	0x9ae63330342d1696ec71055df3dd4daab5cd848a
Contract's current owner address	0x9ae63330342d1696ec71055df3dd4daab5cd848a



Daddy Shark Overview

Project Details:

Daddy Shark Token will be a BSC Rewards token with the goal of expanding the market share of the BabyShark Token ecosystem. This is achieved by allowing holders to choose any BSC token they want as a reward. Not only can you choose which token you get rewarded in, but you are able to change that token at any time.
(Daddy Shark is a subsidiary of BabyShark Token)

Tokenomics:

Starting Supply: 1,000,000,000,000,000 (1 Quadrillion)

7% Rewards

3% Operations

2% Buybacks

2-4% Sliding Scale Liquidity Fee.

Team Review:

DaddyShark as a subsidiary of BabyShark token has a team of at least 22 personnel, which include Blockchain Developers, Web developers, Marketers, Moderators, Designers and Ambassadors.

The review identified a strong level of competence in the team and provides a good degree of confidence in the project.



CONTRACT FUNCTIONS DETAILS

FUNCTIONS (PUBLIC)

1. airdropToWallets
2. approve
3. buyBackTokensWithNoFees
4. claim
5. decreaseAllowance
6. disableTransferDelay
7. excludeFromDividends
8. excludeFromFees
9. excludeMultipleAccountsFromFees
10. includeInDividends
11. increaseAllowance
12. processDividendTracker
13. renounceOwnership
14. setAutomatedMarketMakerPair
15. setBlacklistToken
16. setRewardToken
17. setRewardTokenWithCustomAMM
18. setWhiteListAMM
19. transfer



Continued

20.transferFrom
21.transferOwnership
22.unsetRewardToken
23.updateBuyBackWallet
24.updateClaimWait
25.updateDividendTokensMinimum
26.updateDividendTracker
27.updateDividendUniswapV2Router
28.updateFees

-
bnbRewardPerc
liquidityPerc
operationsPerc
buyBackPerc

-
29.updateGasForProcessing
30.updateLiquidityWallet
31.updateMaxTxn
32.updateOperationsWallet
33.updateSwapTokensAtAmount
34.updateUniswapV2Router



Function Risks

Upon review of Smart Contract Coding and Functions available for the Owner to change Watchtower is satisfied that no malicious coding has been found.

Note: It is necessary to advise that even though we believe the project to be genuine that the Tax fees can be manipulated to high amounts making it difficult or impossible to sell tokens. This is evident in almost all rewards tokens that are un-renounced however having a doxxed team with a good history alleviates the concern or risk of this occurring with this project.



Imported Libraries / Interfaces

- Context
- Ownable
- IERC20
- IERC20 Metadata
- DividendPayingTokenOptionalInterface
- DividendPayingTokenInterface
- SafeMathInt
- SafeMathUint
- SafeMath
- ERC20
- DividendPayingToken (<https://github.com/roger-wu>) + edits
- IUniswapV2Router01
- IUniswapV2Router02
- IUniswapV2Factory
- IUniswapV2Pair

Overview

1. ADDITION OF COMMENTS:	10
2. CALL STACK DEPTH ATTACK:	10
3. TIME STAMP DEPENDENCY:	10
4. PARTY MULTISIG BUG:	10
5. USE OF LIBRARIES/DEPENDENCIES (FROM TRUSTED SOURCES):	10
a. TRANSACTION-ORDERING DEPENDENCY:	10
6. ACCESS CONTROL AND AUTHORIZATION:	10
7. REENTRANCY ATTACKS:	10
8. ERC/BEP STANDARD VIOLATIONS:	10
9. USAGE OF VISIBILITY LEVELS:	10



ISSUES CHECKING STATUS



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.	Low issues
10. Methods execution permissions.	Passed



Issue description	Checking status
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 Issues



Medium Severity Issues

1 Medium Severity issue found.

BNB transfers with a low gas limit:

_withdrawDividendOfUser() function of DividendPayingToken contract transfers BNB via .call{value, gas} method with 3000 of gas limit.

This relatively small constant may cause problems with future ETH/BSC updates as operation gas costs may change with forks.



Low Severity Issues

4 Low Severity issues found

1. buybackWallet declared as private
2. maxSellTransactionAmount is always applied (buy, sell, transfer between EOA), not only during sells, it should be renamed (ex. maxTxAmount)
3. Lines: 1514- 1519: liquidity, operations and buyback wallets are excluded from fees, so these lines can be removed. Lines 1520-21 already includes them.
4. Line 1191: "DaddyShark: gasForProcessing must be between 200,000 and 500,000" should be: "DaddyShark: gasForProcessing must be between 200,000 and 2,500,000"



CONCLUSION

A Custom Smart Contract has been compiled with numerous functions which conveys good competency from the Daddy Shark development team.

The Smart contract review contains a number low severity issues which do not raise any major concerns.

The Token has not been launched so subsequent tests were unable to be completed.

Token Supply and Liquidity Lock details unavailable until Launch.

Watchtower Scanner will not yield any further results until the token has been launched.

Watchtower note:

Please check the disclaimer above and note, this Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please invest at your own risk.

(<https://www.cryptowatchtower.io/>)

Contact Us

 @Watchtower_WTW

 Watchtower-WTW

 Watchtowercrypto

