

DESSERT  
FINANCE



**BABY ANGEL DUST (\$BAD)**  
**LIGHT AUDIT**

Performed at block **21979634**

PERFORMED BY DESSERT FINANCE  
FOR CONTRACT ADDRESS: **0x3998d546ef53915A073B7932f2A82525cdEaBBd4**

## INITIAL DISCLAIMER

Dessert Finance provides due-diligence project audits for various projects. Dessert Finance in no way guarantees that a project will not remove liquidity, sell off team supply, or otherwise exit scam.

Dessert Finance does the legwork and provides public information about the project in an easy-to-understand format for the common person.

Agreeing to an audit in no way guarantees that a team will not remove *all* liquidity (“Rug Pull”), remove liquidity slowly, sell off tokens, quit the project, or completely exit scam. There is also no way to prevent private sale holders from selling off their tokens. It is ultimately your responsibility to read through all documentation, social media posts, and contract code of each individual project to draw your own conclusions and set your own risk tolerance.

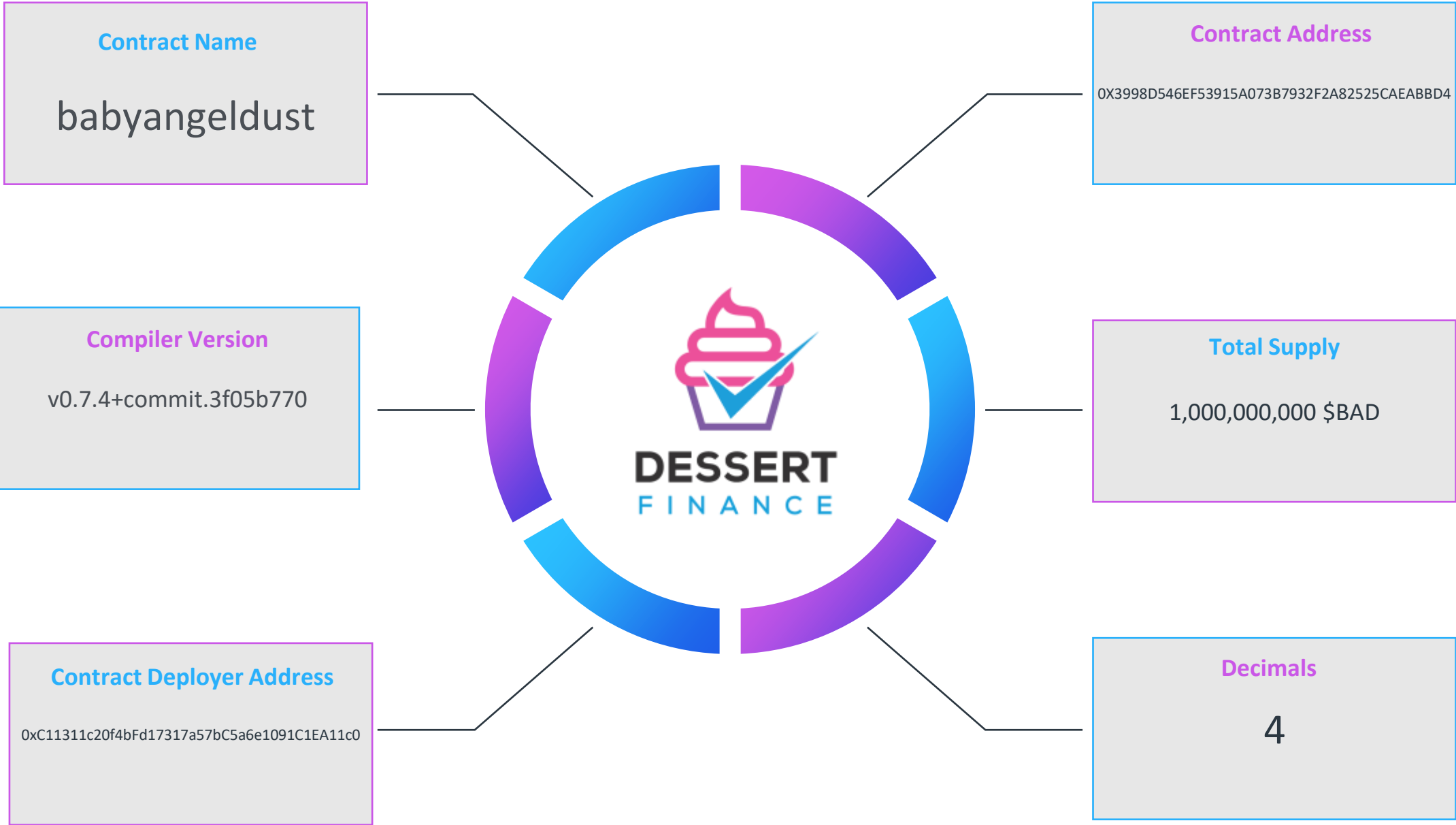
Dessert Finance in no way takes responsibility for any losses, nor does Dessert Finance encourage any speculative investments. The information provided in this audit is for information purposes only and should not be considered investment advice. Dessert Finance does not endorse, recommend, support, or suggest any projects that have been audited. An audit is an informational report based on our findings, We recommend you do your own research, we will never endorse any project to invest in.

# Table of Contents



1. Contract Code Audit – Token Overview
2. BEP-20 Contract Code Audit – Overview
3. BEP-20 Contract Code Audit – Vulnerabilities Checked
4. Disclaimers

# Contract Code Audit – Token Overview





# BEP-20 Contract Code Audit – Overview

Dessert Finance was commissioned to perform an audit on BABY ANGEL DUST (\$BAD)

```
/**
 *Submitted for verification at BscScan.com on 2022-09-27
 */
//SPDX-License-Identifier: MIT

pragma solidity ^0.7.4;
library SafeMath {
    function add(uint256 a, uint256 b) internal pure returns (uint256) {
        uint256 c = a + b;
        require(c >= a, "SafeMath: addition overflow");

        return c;
    }
    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
        return sub(a, b, "SafeMath: subtraction overflow");
    }
    function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
        require(b <= a, errorMessage);
        uint256 c = a - b;

        return c;
    }
    function mul(uint256 a, uint256 b) internal pure returns (uint256) {
        if (a == 0) {
            return 0;
        }
        uint256 c = a * b;
        require(c / a == b, "SafeMath: multiplication overflow");

        return c;
    }
    function div(uint256 a, uint256 b) internal pure returns (uint256) {
        return div(a, b, "SafeMath: division by zero");
    }
    function div(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
        // Solidity only automatically asserts when dividing by 0
        require(b != 0, errorMessage);
        uint256 c = a / b;
        // assert((a == 0 ? c == a * b) : There is no case in which this doesn't hold);

        return c;
    }
}

/**
 * BSC20 standard interface
 */
interface BSC20 {
    function totalSupply() external view returns (uint256);
    function decimals() external view returns (uint8);
    function symbol() external view returns (string memory);
    function name() external view returns (string memory);
    function getOwner() external view returns (address);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address recipient, uint256 amount) external returns (bool);
    function allowance(address owner, address spender) external view returns (uint256);
}
```

## Contract Address

0x3998d546Ef53915A073B7932f2A82525caEaBBd4

## TokenTracker

BABY ANGEL DUST (\$BAD)

## Contract Creator

0xc11311c20f4bfd17317a57bc5a6e1091c1ea11c0

## Source Code

Contract Source Code Verified

## Contract Name

babyangeldust

## Other Settings

default evmVersion, MIT

## Compiler Version

v0.7.4+commit.3f05b770

## Optimization Enabled

No with 200 runs

Code is truncated to fit the constraints of this document.

[The code in its entirety can be viewed here.](#)

# BEP-20 Contract Code Audit – Vulnerabilities Checked

Vulnerability Tested	Scan	Result
Compiler Errors	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	✓ Low / No Risk
Integer Overflow	Complete	✓ Low / No Risk
Integer Underflow	Complete	✓ Low / No Risk
Floating Pragma	Complete	✓ Low / No Risk
Timestamp Dependency for Crucial Functions	Complete	✓ Low / No Risk
Exposed _Transfer Function	Complete	✓ Low / No Risk
Transaction-Ordering Dependency	Complete	✓ Low / No Risk
Unchecked Call Return Variable	Complete	✓ Low / No Risk
Use of Deprecated Functions	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	✓ Low / No Risk
State Variable Default Visibility	Complete	✓ Low / No Risk

The contract code is **verified** on BSCScan.

The vulnerabilities listed above were not found in the token's Smart Contract.

# Contract Code Audit – Contract Ownership

Contract Ownership has not been renounced at the time of Audit



The contract ownership is not currently renounced.

We have placed the contract owner address below for your viewing:

[0xc11311c20f4bfd17317a57bc5a6e1091c1ea11c0](https://www.etherbase.net/etherbase-token/contract-ownership)

The address above has authority over the ownable functions within the contract.

This allows the owner to call certain functions within the contract. Any compromise to the owner wallet may allow these privileges to be exploited.

We recommend:

- Establishing a Time-Lock with reasonable latency
- Assignment of privileged roles to multi-signature wallets

# Contract Code Audit – Owner Accessible Functions

Function Name	Parameters	Visibility	Audit Notes
authorize	address adr	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
unauthorize	address adr	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
transferOwnership	address payable adr	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setMaxWalletPercent	uint256 maxWallPercent	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
tradingStatus	bool _status	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
cooldownEnabled	bool _status, uint8 _interval	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
airdrop	address from, address[] calldata addresses, uint256[] calldata tokens	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.

The functions listed above can be called by the contract owner.

If contract ownership has been renounced there is no way for the above listed functions to be called.



# Disclaimer



The opinions expressed in this document are for general informational purposes only and are **not intended to provide specific advice or recommendations for any individual or on any specific investment**. It is only intended to provide education and public knowledge regarding projects. This audit is only applied to the type of auditing specified in this report and the scope of given in the results. Other unknown security vulnerabilities are beyond responsibility. Dessert Finance only issues this report based on the attacks or vulnerabilities that already existed or occurred before the issuance of this report. For the emergence of new attacks or vulnerabilities that exist or occur in the future, Dessert Finance lacks the capability to judge its possible impact on the security status of smart contracts, thus taking no responsibility for them. The smart contract analysis and other contents of this report are based solely on the documents and materials that the contract provider has provided to Dessert Finance or was publicly available before the issuance of this report (issuance of report recorded via block number on cover page), if the documents and materials provided by the contract provider are missing, tampered, deleted, concealed or reflected in a situation that is inconsistent with the actual situation, or if the documents and materials provided are changed after the issuance of this report, Dessert Finance assumes no responsibility for the resulting loss or adverse effects. Due to the technical limitations of any organization, this report conducted by Dessert Finance still has the possibility that the entire risk cannot be completely detected. Dessert Finance disclaims any liability for the resulting losses.

Dessert Finance provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Even projects with a low risk score have been known to pull liquidity, sell all team tokens, or exit-scam. Please exercise caution when dealing with any cryptocurrency related platforms.

The final interpretation of this statement belongs to Dessert Finance.

Dessert Finance highly advises against using cryptocurrencies as speculative investments and they should be used solely for the utility they aim to provide.



# Thank You

DESSERT FINANCE LIGHT AUDIT HAS BEEN COMPLETED FOR DESSERTSWAP (DSRT)  
THIS AUDIT IS ONLY VALID IF VIEWED ON [HTTPS://WWW.DSSERTSWAP.FINANCE](https://www.dessertswap.finance)

[www.dessertswap.finance](http://www.dessertswap.finance)  
<https://t.me/dessertswap>