

DESSERT
FINANCE



Polaris (Polaris)

BEP-20 Audit

Performed at block **11766786**

PERFORMED BY DESSERT FINANCE
FOR CONTRACT ADDRESS: 0x0BCd8bCc1411bc19747D0AB2f7a8b3a740b549D6

INITIAL DISCLAIMER

Dessert Finance provides due-diligence project audits for various BSC 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 a project audit can be seen as a sign of confidence and is generally the first sign of trust for a project, but in no way guarantees that a team will not remove *all* liquidity (“Rug Pull”), sell off tokens, 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.

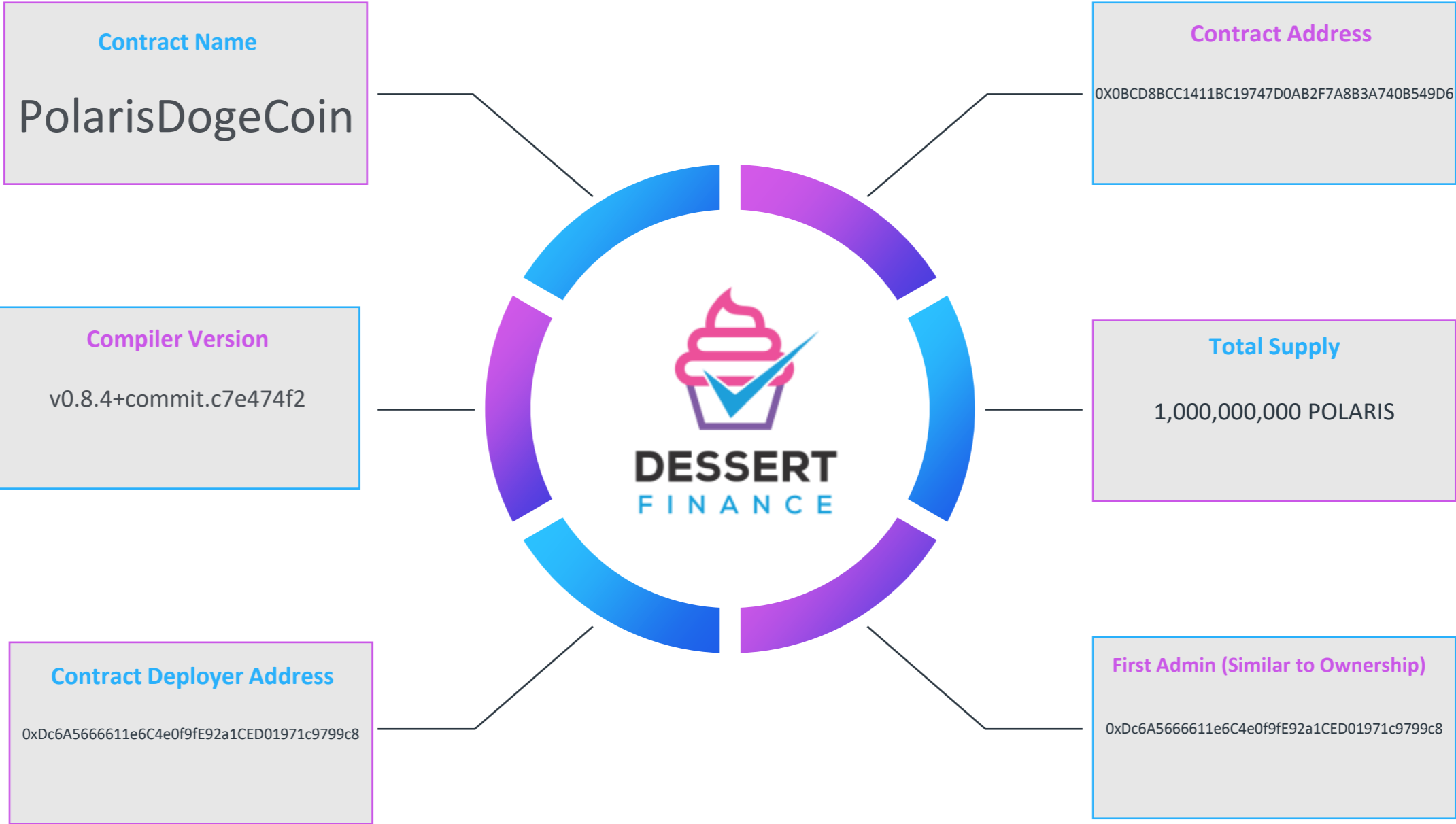
Dessert Finance in no way takes responsibility for any losses, nor does Dessert Finance encourage any speculative investments. The information provided in this audit is for information purposes only and should not be considered investment advice.

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. Contract Code Audit – Contract Ownership
5. Liquidity Ownership – Locked / Unlocked
6. Contract Code Audit – Mint Functions
7. Contract Transaction Fees
8. Website Overview
9. Social Media
10. Top Token Holders/Wallets
11. Location Audit
12. Review of Team
13. Roadmap
14. Disclaimers

Contract Code Audit – Token Overview



BEP-20 Contract Code Audit – Overview

Dessert Finance was commissioned to perform an audit on Polaris (Polaris)

```
Submitted for verification at BscScan.com on 2021-10-07
/
/ File: @ponicappelin/contracts/utlis/Address.sol
/ SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

/**
 * @dev Collection of functions related to the address type
 */
library Address {
    /**
     * @dev Returns true if "account" is a contract.
     *
     * [IMPORTANT]
     *
     * It is unsafe to assume that an address for which this function returns
     * true is an externally-owned account (EOA) and not a contract.
     *
     * Among others, "isContract" will return true for the following
     * types of addresses:
     *
     * - an externally-owned account
     * - a contract in construction
     * - an address where a contract will be created
     * - an address where a contract lived, but was destroyed
     *
     */
    function isContract(address account) internal view returns (bool) {
        // This method relies on extcodesize, which returns 0 for contracts in
        // construction, since the code is only stored at the end of the
        // constructor execution.

        uint256 size;
        assembly {
            size := extcodesize(account)
        }
        return size > 0;
    }

    /**
     * @dev Replacement for Solidity's "transfer": sends "amount" wei to
     * "recipient", forwarding all available gas and reverting on errors.
     *
     * https://eips.ethereum.org/EIPs/eip-1884[EIP1884] increases the gas cost
     * of certain opcodes, possibly making contracts go over the 2300 gas limit
     * imposed by "transfer", making those unable to receive funds via
     * "transfer". {sendValue} removes this limitation.
     *
     * https://diligence.consensys.net/posts/2018/09/stop-using-soliditys-transfer-now/[learn more].
     *
     * [IMPORTANT] because control is transferred to "recipient", care must be
     * taken to not create reentrancy vulnerabilities. Consider using
     * {ReentrancyGuard} or the
     * https://solidity.readthedocs.io/en/v0.5.11/security-considerations.html#use-the-checks-effects-interactions-pattern[checks-effects-interactions pattern].
     */
    function sendValue(address payable recipient, uint256 amount) internal

```

Contract Address

0x0BCd8bCc1411bc19747D0AB2f7a8b3a740b549D6

TokenTracker

Polaris (Polaris)

Contract Creator

0xdc6a5666611e6c4e0f9fe92a1ced01971c9799c8

Source Code

Contract Source Code Verified

Contract Name

PolarisDogeCoin

Other Settings

default evmVersion, None

Compiler Version

v0.8.4+commit.c7e474f2

Optimization Enabled

Yes 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	AI Scan	Human Review	Result
Integer Overflow	Complete	Complete	✓ Low / No Risk
Integer Underflow	Complete	Complete	✓ Low / No Risk
Correct Token Standards Implementation	Complete	Complete	✓ Low / No Risk
Timestamp Dependency for Crucial Functions	Complete	Complete	✓ Low / No Risk
Exposed _Transfer Function	Complete	Complete	✓ Low / No Risk
Transaction-Ordering Dependency	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Variable	Complete	Complete	✓ Low / No Risk
Use of Deprecated Functions	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
State Variable Default Visibility	Complete	Complete	✓ Low / No Risk
Deployer Can Access User Funds	Complete	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 Using Admin Roles for Access Control



This contract does not use the “OnlyOwner” modifier.

POLARIS provides access control through roles.

The highest level role is the **DEFAULT_ADMIN_ROLE (0x00)**.

There may be more than one member of the DEFAULT_ADMIN_ROLE at any given time. The first and only DEFAULT_ADMIN_ROLE was given to the following address at the time of audit:

[0xDc6A5666611e6C4e0f9fE92a1CED01971c9799c8](https://www.etherbase.net/etherbase-account/0xDc6A5666611e6C4e0f9fE92a1CED01971c9799c8)

20. getRoleMember

role (bytes32)

0x00

index (uint256)

0

Query

↳ address

[getRoleMember method Response]

» address : 0xDc6A5666611e6C4e0f9fE92a1CED01971c9799c8

Contract Code Audit – Contract Ownership

Contract Using Admin Roles for Access Control



DEFAULT_ADMIN_ROLE Functions

1. removeSniper
2. setSniperProtectionEnabled
3. addBotToList
4. enableTrading
5. setMaxTxPercent
6. setMaxWalletPercent
7. setSwapAndLiquifyEnabled
8. excludeFromDividends
9. excludeFromMaxWallet
10. includeInMaxWallet
11. excludeFromMaxTx
12. includeInMaxTx
13. excludeFromFee
14. includeInFee
15. setDxSaleAddress
16. setAutomatedMarketMakerPair
17. updateClaimWait
18. withdrawLockedETH (withdraw bnb accidentally sent to this contract)
19. withdrawLockedTokens (tokens that are not supposed to be in the contract)
20. setMarketingWallet
21. setLiquidityWallet
22. updateDividendTracker
23. changeFees

Liquidity Ownership – Locked / Unlocked

No locked liquidity information has been found.



This page will contain links to locked liquidity for the project if we are able to locate that information. Locked liquidity information was not found on the project's website.

Contract Code Audit – Mint Functions

This Contract Cannot Mint New POLARIS Tokens.



We do understand that sometimes mint functions are essential to the functionality of the project.

A mint function was not found in the contract code.

Contract Transaction Fees

At the time of Audit the transaction fees (“tax”) listed below are the fees associated with trading. These fees are taken from every buy and sell transaction unless otherwise stated.

Marketing Tax

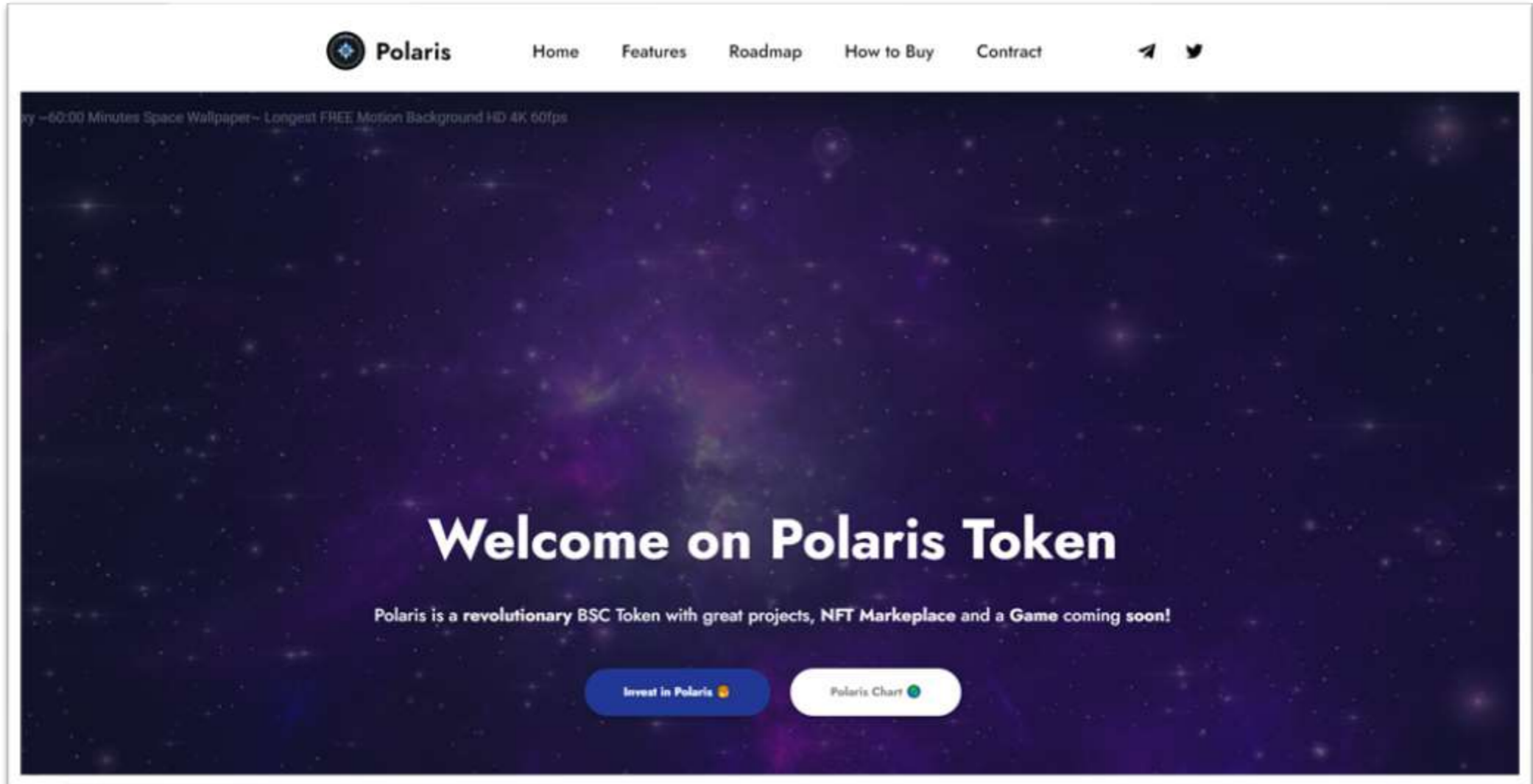
To aim **big influencers**, we need a big wallet, that’s why the **3%** goes in the **Marketing wallet**

Huge Auto LP

Never running out of funds, we **decided** to give the Liquidity Pool the **15%** of the current taxes

Website Part 1 – Overview

www.polarisbsc.com



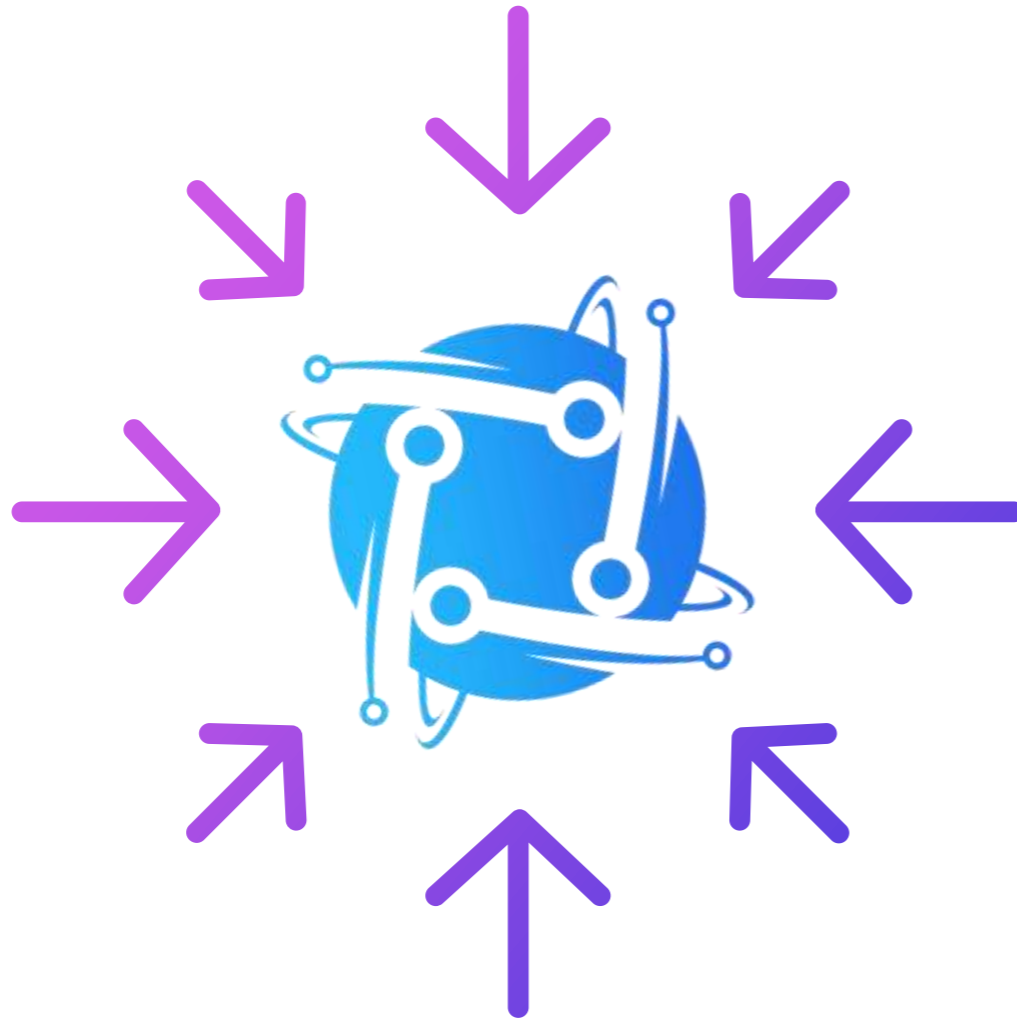
Above images are actual snapshots of the current live website of the project.

Website was registered on 10/06/2021, registration expires 10/06/2022.

X This does not meet the 3 year minimum we like to see on new projects.



Website Part 2 – Checklist



- ✓ Mobile Friendly
- ✗ No JavaScript Errors
- ✓ Spell Check
- ✓ SSL Certificate

The website contained some JavaScript errors. No typos, or grammatical errors were present, and we found a valid SSL certificate allowing for access via https.

No additional issues were found on the website.

Website Part 3 – Responsive HTML5 & CSS3

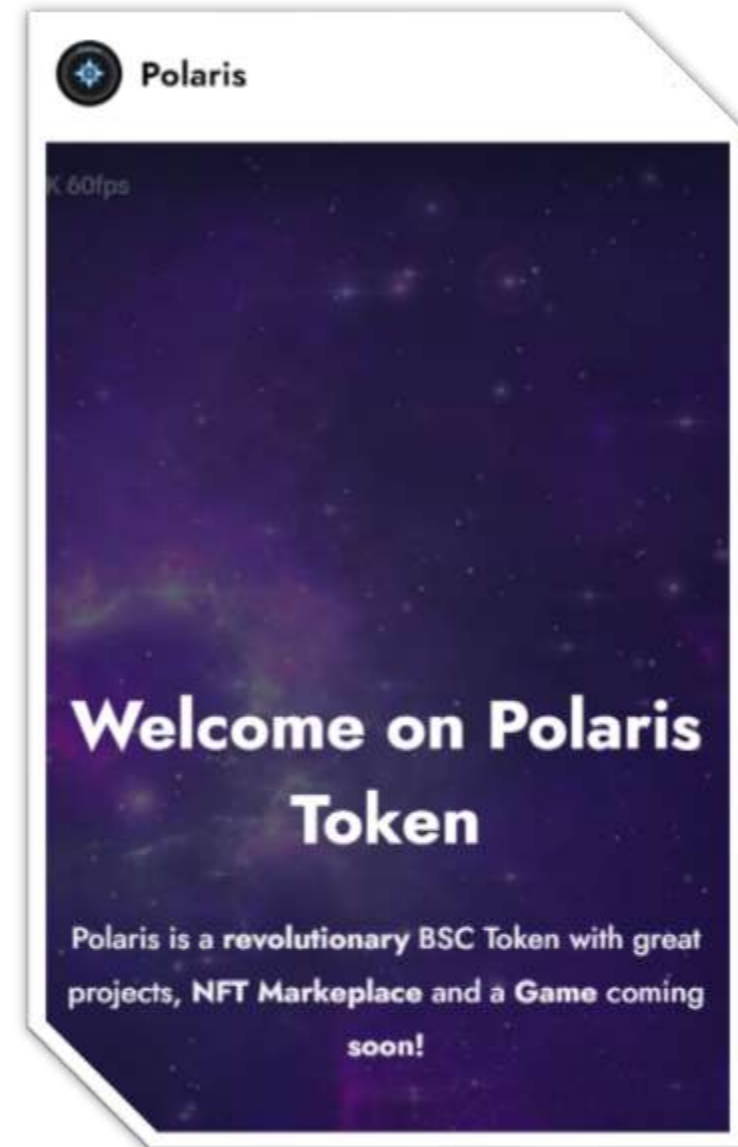
No issues were found on the Mobile Friendly check for the website. All elements loaded properly and browser resize was not an issue. The team has put a considerable amount of thought and effort into making sure their website looks great on all screens.

Some JavaScript errors were found. No issues with loading elements, code, or stylesheets.

```
✖ Failed to load resource: the server responded with a status of 404 ()
  socicon.woff2:1
  status of 404 ()

⚠ jQuery.Deferred exception: Cannot read properties of undefined (reading 'match') TypeError: Cannot read properties of undefined (reading 'match')
    at HTMLIFrameElement.<anonymous> (https://www.polarisbsc.com/assets/theme/js/script.js:1:13554)
    at Function.each (https://www.polarisbsc.com/assets/web/assets/jquery/jquery.min.js:2:2976)
    at S.fn.init.each (https://www.polarisbsc.com/assets/web/assets/jquery/jquery.min.js:2:1454)
    at HTMLDocument.<anonymous> (https://www.polarisbsc.com/assets/theme/js/script.js:1:13468)
    at e (https://www.polarisbsc.com/assets/web/assets/jquery/jquery.min.js:2:30005)
    at t (https://www.polarisbsc.com/assets/web/assets/jquery/jquery.min.js:2:30307) undefined

✖ Uncaught TypeError: Cannot read properties of undefined (reading 'match')
    at HTMLIFrameElement.<anonymous> (script.js:1)
    at Function.each (jquery.min.js:2)
    at S.fn.init.each (jquery.min.js:2)
    at HTMLDocument.<anonymous> (script.js:1)
    at e (jquery.min.js:2)
    at t (jquery.min.js:2)
```



Website Part 4 (GWS) – General Web Security



SSL CERTIFICATE

A valid SSL certificate was found. Details are as follows:

Offered to: polarisbsc.com

Issued by: Cloudflare Inc

Valid Until: 10/06/2022



CONTACT EMAIL

A valid contact email was found on the official website. Contact email is listed as shown below:

Contact

N/A



SPAM / MALWARE / POPUPS

No malware found

No injected spam found

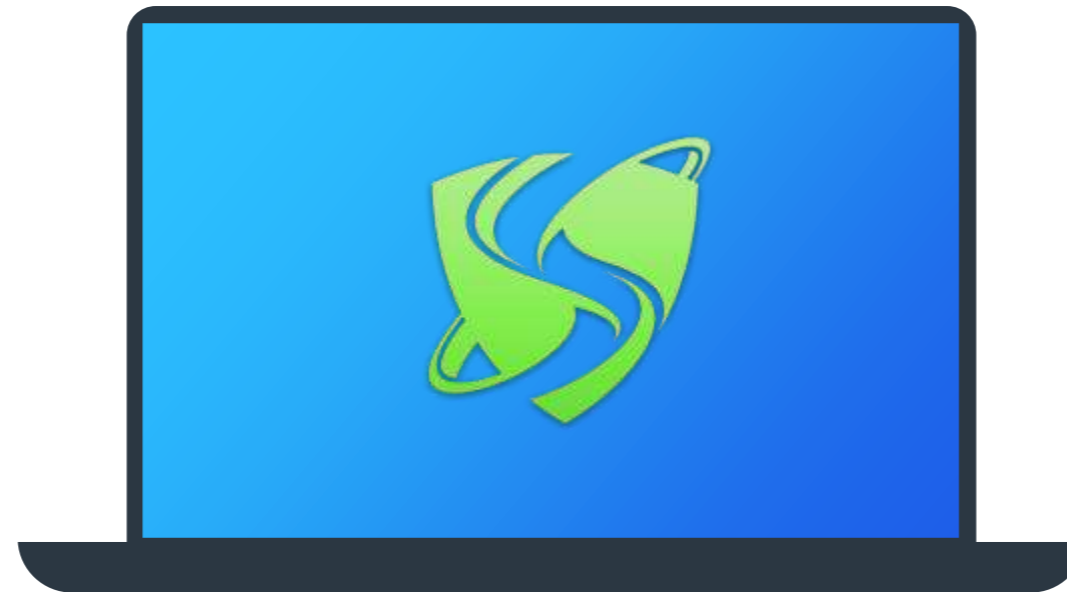
No internal server errors

No popups found

Domain is marked clean by Google, McAfee, Sucuri Labs, & ESET



Social Media



We were able to locate a variety of Social Media networks for the project.

All links have been conveniently placed below.



[Twitter](#)



[Telegram](#)

X At least 3 social media networks were found.

Top Token Holders

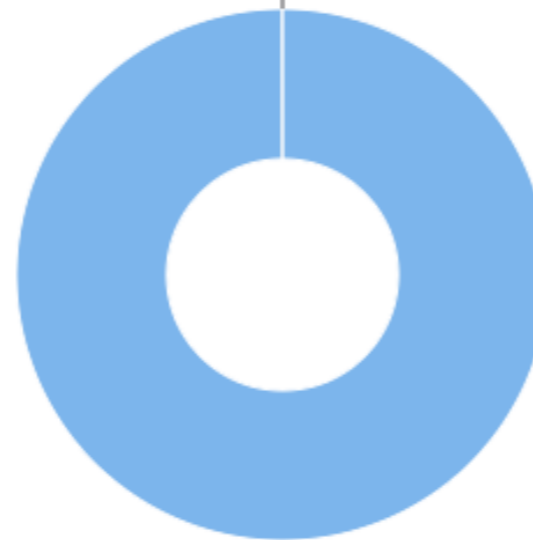
The entire supply was in one wallet at the time of audit. We expect this to change as the project goes through initial distribution phases. Please use the link below to view the most up-to-date holder information.

[Click here to view the most up-to-date list of holders](#)

Polaris Top 100 Token Holders

Source: BscScan.com

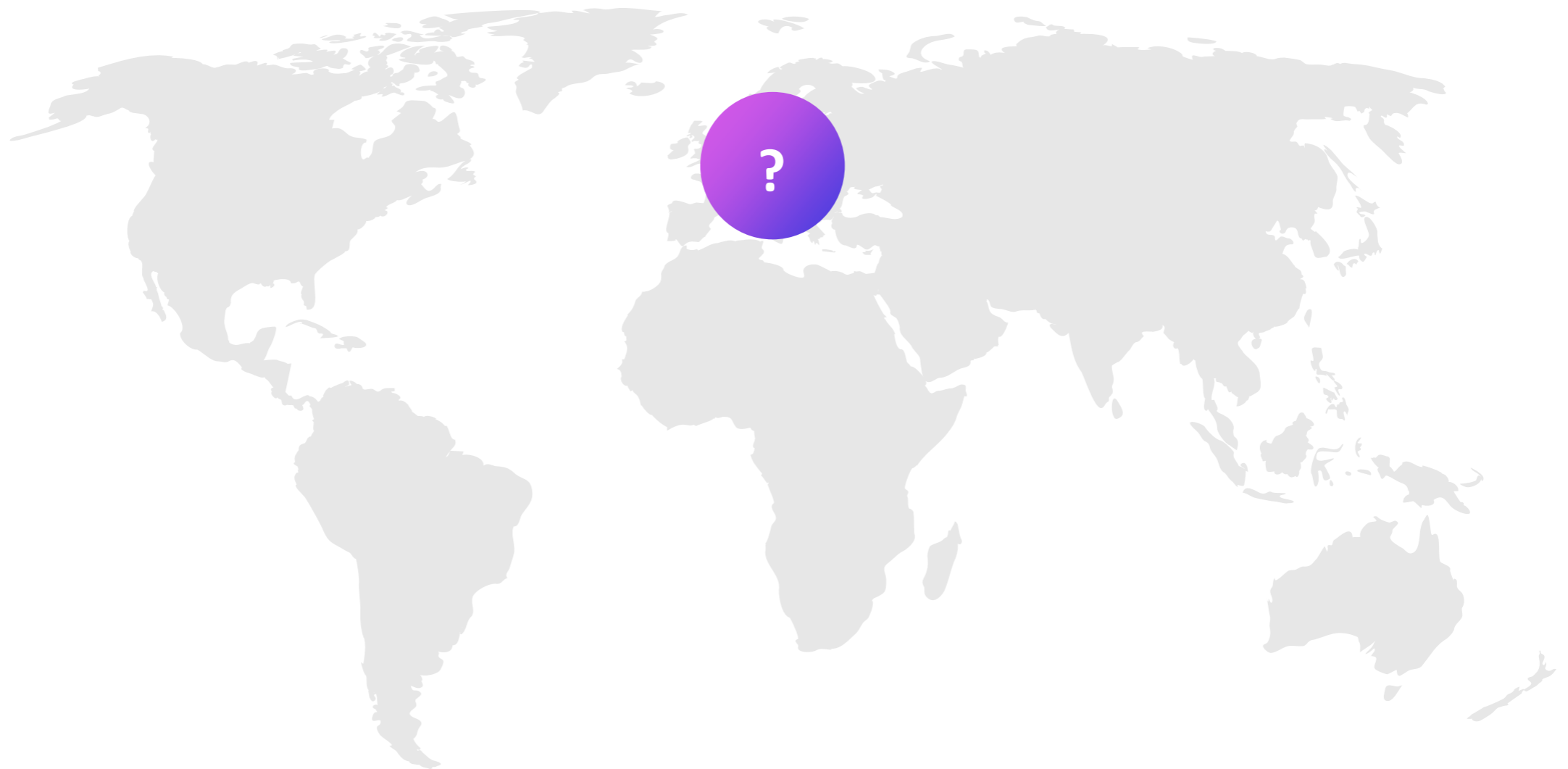
OTHER ACCOUNTS



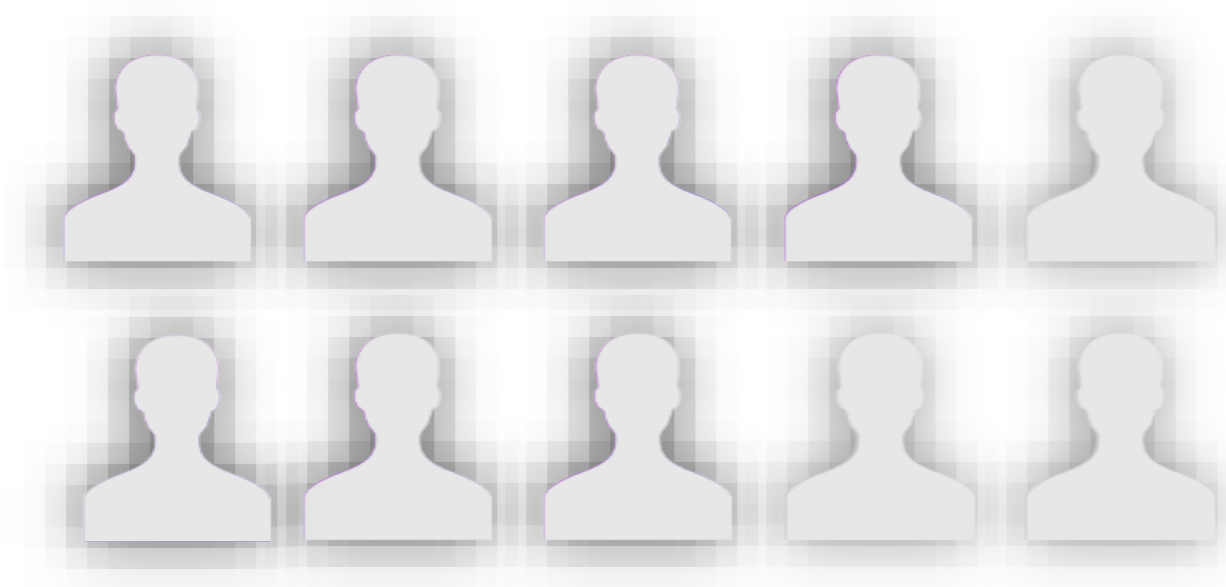
`0xdc6a5666611e6c4e0f9fe92a1ced01971c9799c8`

Location Audit

We were unable to identify a primary location for the project at this time or a location has not been declared.



Team Overview



We are unable to find any information about the team on the website at this time. Projects may choose to stay anonymous for a myriad of reasons.

Roadmap

A roadmap was found on the official website, we have conveniently placed it on this page for your viewing.



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 BSC 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 PROJECT AUDIT HAS BEEN COMPLETED FOR POLARIS (POLARIS) 1 DSRT HAS BEEN SENT TO AUDITED PROJECT'S CONTRACT ADDRESS FOR VERIFICATION OF THIS AUDIT AT BLOCK NUMBER: **11766786**

www.dessertswap.finance
<https://t.me/dessertswap>