2022

Smart Contract Audit Report

BEP-20 Audit

PERFORMED BY ByteSphere

For PandaFury Contract Address: 0x327c8ec038b7e642766941942a5431c0526d600e

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. 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

01 — Website Overview

02 — BEP-20 Contract Audit

03 — Social Media

04 — Team Response

05 — Token Distribution

06 — Top Token Holders/Wallets

07 — Location Audit

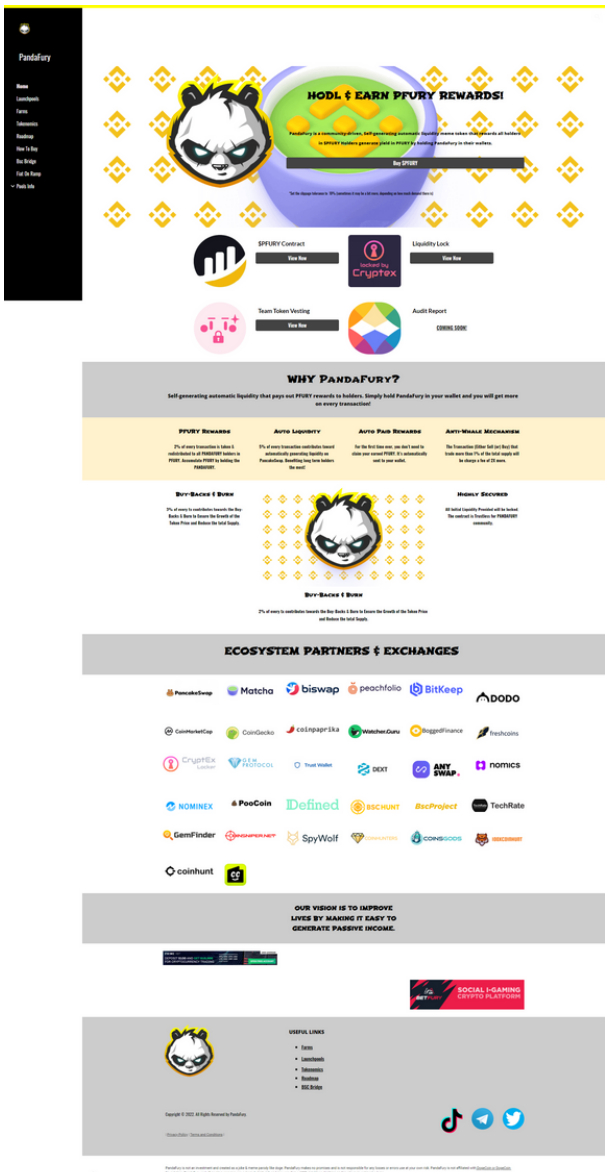
08 — Review of Team

09 — Potential Risk Factors

10 — Roadmap

11 — Disclaimers

Website Part 1 – Overview
www.pandafurytoken.com



Above images are actual snapshots of the current live website of the project.
Website was registered on 05/12/2021, registration expires 05/12/2022.
✓ This does not meet the 3 year minimum we like to see on new projects however we have validated that auto renewal is currently enabled and the inability to purchase multiple years is a limitation with the registrar used.

WEBSITE DESKTOP AND MOBILE VIEW AUDIT

// YOUR NFP NAME

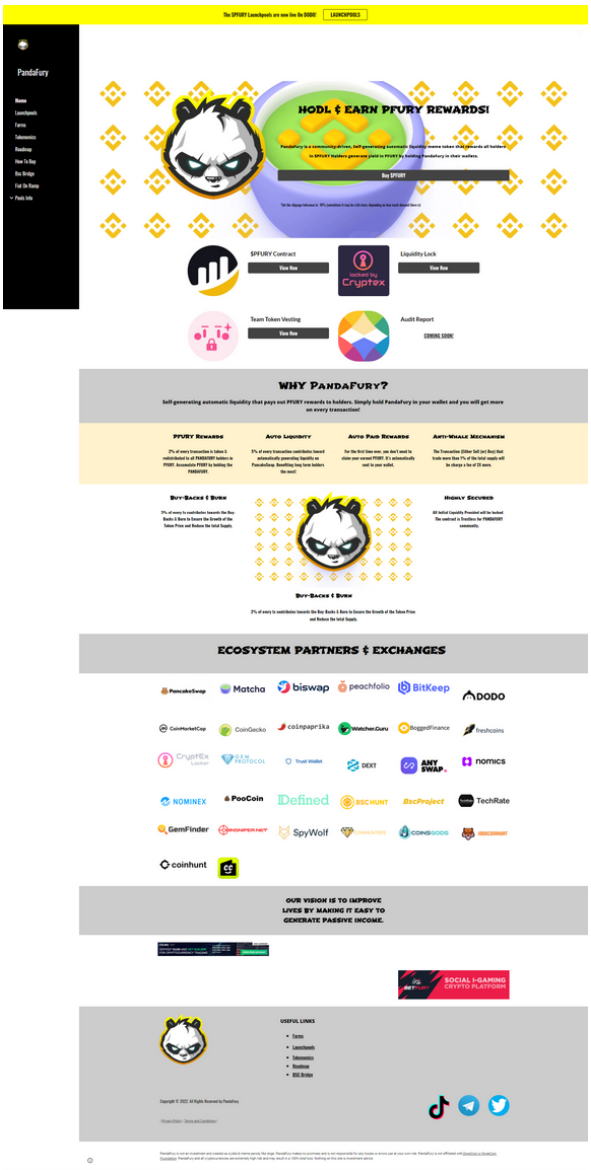
Website Part 2 – Checklist

- Responsive
- No JavaScript Errors
- Spell Check
- SSL Certificate

The website contained no 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 responsive 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.
No issues with loading elements, code, or stylesheets were present.



Website Part 4 (GWS) – General Web Security

SSL CERTIFICATE

A valid SSL certificate was found. Details are as follows:
Offered to: babydogecoin.com
Issued by: R3
Valid Until: 08/10/2021

CONTACT EMAIL

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

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

BEP-20 Contract Audit – Common Vulnerabilities

```
pragma solidity 0.6.11;

contract VendingMachine {

    // Declare state variables of the contract
    address public owner;
    mapping (address => uint) public cupcakeBalances;

    // When 'VendingMachine' contract is deployed:
    // 1. set the deploying address as the owner of the contract
    // 2. set the deployed smart contract's cupcake balance to 100
    constructor() public {
        owner = msg.sender;
        cupcakeBalances[address(this)] = 100;
    }

    // Allow the owner to increase the smart contract's cupcake balance
    function refill(uint amount) public {
        require(msg.sender == owner, "Only the owner can refill.");
        cupcakeBalances[address(this)] += amount;
    }

    // Allow anyone to purchase cupcakes
    function purchase(uint amount) public payable {
        require(msg.value >= amount * 1 ether, "You must pay at least 1
ETH per cupcake");
        require(cupcakeBalances[address(this)] >= amount, "Not enough
cupcakes in stock to complete this purchase");
        cupcakeBalances[address(this)] -= amount;
        cupcakeBalances[msg.sender] += amount;
    }
}
```

- Integer Underflow
- Integer Overflow
- Callstack Depth Attack
- Timestamp Dependency
- Parity Multisig Bug
- Transaction-Ordering Dependency

The contract code is verified on BSCScan.
Common vulnerabilities were not found in the token's Smart Contract as shown above.

Social Media

We were able to locate a variety of Social Media networks for the project including Twitter, Telegram, Reddit, and Instagram. All links have been conveniently placed below.

Social and Web – Final Thoughts & Suggestions for Improvement

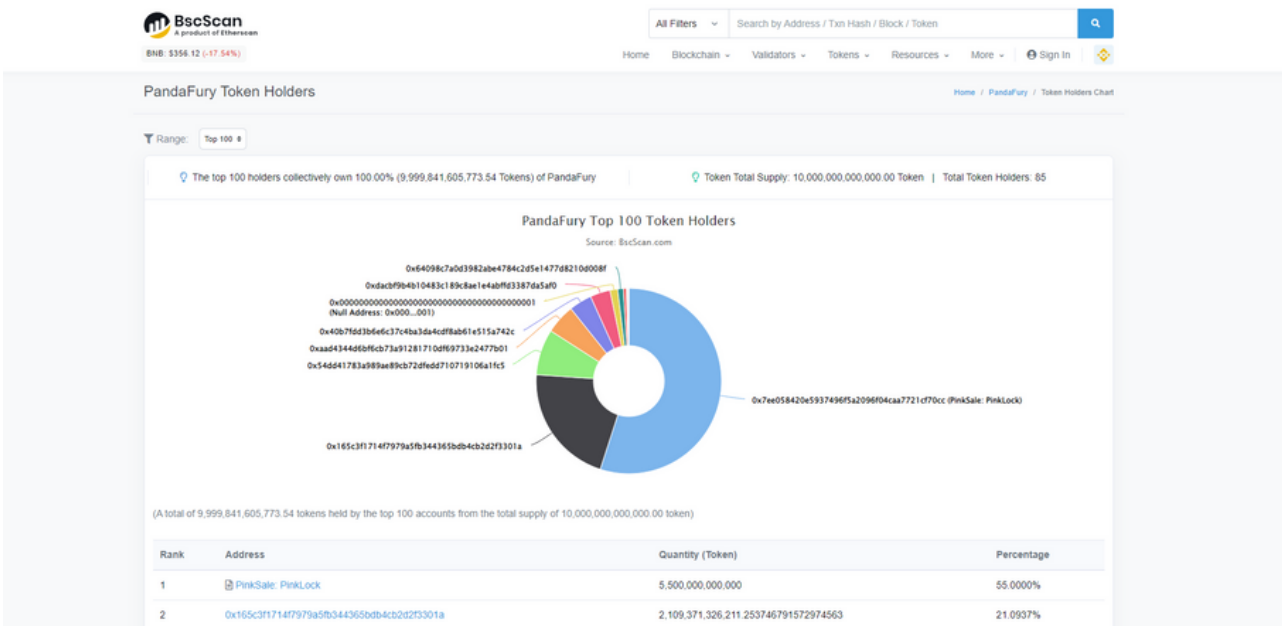
SOCIAL MEDIA
– SUGGESTIONS FOR IMPROVEMENT

We were able to track down multiple social media channels for the project. Social Media channels included Twitter, Telegram, Reddit, and Instagram. All social media channels had a healthy amount of activity. While there is a reddit account for Baby Doge Coin, it is important to note that this is not a subreddit. We were able to locate a corresponding subreddit.

It is important to note that there is an 10% fee on EVERY transaction including buys and sells. 5% goes to providing liquidity, and 5% is distributed to the token holders.

TOP TOKEN HOLDERS

The top token holders at the time of the audit are shown below.



1. Burn Address– the top token holder was a the burn address holding 28.7% of the total supply. These tokens are permanently removed from circulation.
2. 0xa4a6db60a345e40f389792952149b2d1255b9542– the 2nd largest holder was a wallet containing 9.9% of the supply. This is a team-controlled wallet intended to be used for charity and marketing.
3. 0xeaed594b5926a7d5fbbc61985390baaf936a6b8d– the 3rd largest holder was a contract containing 9.5% of the supply. We are told this wallet is a contract of locked tokens.

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.

Potential Signs of Risk

1 YEAR DOMAIN REGISTRATION

PROJECT HAS COMMON USE-CASE (REFLECT TOKEN)

The above listed are the top 2 risk indicators of the project. These are by no means assigning the project as a risky project. Every project will have the top risk indicators posted. It is crucial to note that some may be more important than others.

POTENTIAL SIGNS OF CONFIDENCE

TEAM HAS BEEN VERY RESPONSIVE IN ADDRESSING QUESTIONS

TRANSPARENT FEE STRUCTURE

SELF IDENTIFYING MEME

TRANSPARENT WALLET FOR CHARITY CONTRIBUTIONS

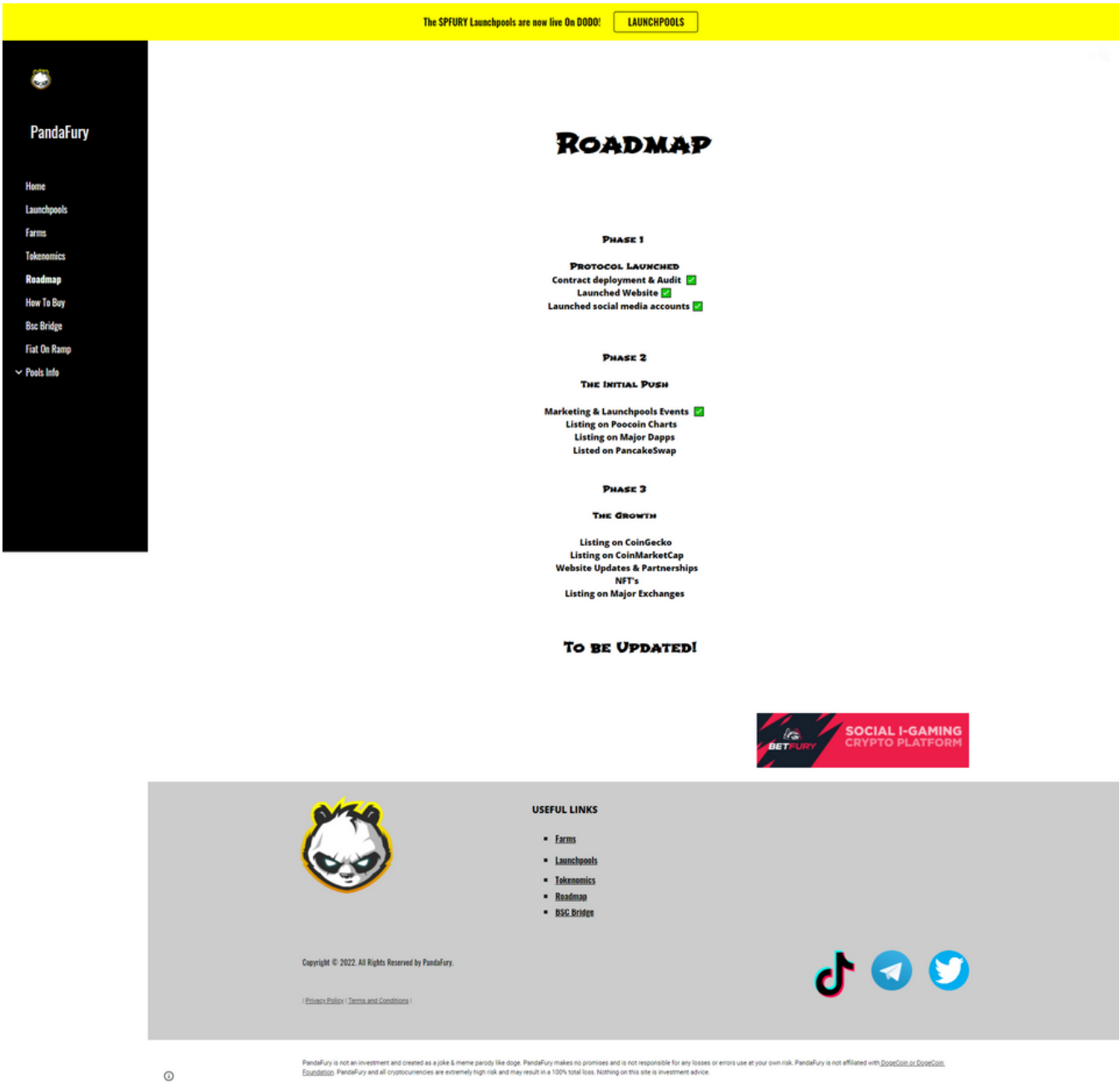
SSL CERTIFICATE WAS FOUND AND VALID

ACTIVE SOCIAL MEDIA PRESENCE

The above listed are the top 6 confidence indicators of the project. These are by no means assigning the project as a confident project. Every project will have the top 6 confidence indicators posted. It is crucial to note that some may be more important than others.

ROADMAP

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



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.