



Royalproof

Security Audit Report



Completed on

30,01,2023

royalproof.net



OVERVIEW

This audit has been prepared for **BabyShinja** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal ”

- RoyalProof Team -



TABLE OF CONTENTS

OVERVIEW	2
TABLE OF CONTENTS	3
PROJECT DESCRIPTION	4
CONTRACT INFO	5
OUR CONTRACT REVIEW PROCESS	6
CURRENT STATS	7
TOKEN TRANSFERS STATS	8
SMART CONTRACT STATS	8
FEATURED WALLETS	9
VULNERABILITY CHECK	10
THREAT LEVELS	11
TOKENOMICS:	14
WEBSITE	15
SOCIAL MEDIA& ONLINE PRESENCE	16
DISCLAIMER	18



PROJECT DESCRIPTION

According to their website:

BabyShinja token was born from team's love of Shibnobi/Shinja. BabyShinja is a community driven decentralized meme token with a dedicated team, pushing and developing behind the scenes to make this the biggest Baby coin of 2022!

Release Date: Presale starts on Aug. 04, 2022

Category: Meme coin



CONTRACT INFO

Token Name	BabyShinja
Symbol	BSHINJA
Contract Address	0x6950Bf7f33acaA6fE0ED91fC5982491beB251c8A
Network	Binance Smart Chain
Language	Solidity
Deployment Date	04, Aug, 2022
Verified?	Yes
Total Supply	1,000,000,000,000,000
Status	Launched

TAXES

Buy Tax	10 %
Sell Tax	10 %



Our Contract Review Process

The contract review process pays special attention to the following:

Testing the smart contracts against both common and uncommon vulnerabilities

- ❖ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ❖ Ensuring contract logic meets the specifications and intentions of the client.
- ❖ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ❖ Thorough line-by-line manual review of the entire codebase by industry experts.

- ❖ Blockchain security tools used:
 - ✓ Open Zeppelin
 - ✓ Mythril
 - ✓ Solidity Compiler
 - ✓ Hardhat



CURRENT STATS

(As of Jan 30, 2023)

Status: Launched

Liquidity: Not added yet

Burn: No burnt tokens

MaxTxAmount: 20,000,000,000,000

DEX: PancakeSwap

LP Address(es):



TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	10000000000000000 BSHINJA
Median Transfer Amount	10000000000000000 BSHINJA
Average Transfer Amount	10000000000000000 BSHINJA
First transfer date	2022-08-04
Last transfer date	2022-08-04
Days token transferred	1

SMART CONTRACT STATS

Calls Count	2
External calls	2
Internal calls	0
Transactions count	2
Uniq Callers	1
Days contract called	1
Last transaction time	2022-08-04 08:14:50 UTC
Created	2022-08-04 07:58:08 UTC
Create TX	0x2eb66df977541642f3524cce9da3e13c0078b18ac11ff379efc323f100438975
Creator	0x3cb5b41ba477da4ea403ce2c667b7bd292130f8b



FEATURED WALLETS

Owner address	Ox3cb5b41ba477da4ea403ce2c667b7bd292130f8b
Auto liquidity receiver	Same as owner
Marketing wallet	Oxbb36079bd916df0fc0504bdc35472ae45e1f4719
Dev wallet	Oxfab30b3f641063dc73924e4b063eOdffd412d7c9
LP address	Liquidity not added yet

*Address can be changed in future

TOP 3 UNLOCKED WALLETS

- **100%** same as owner

*Tokens are not distributed yet



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer Overflow and Underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk-free factor.



THREAT LEVELS

- **Medium Risk**

Owner can change buy and sell fees up to 25%.
Combined buy+sell = 50%.

```
function changeFees(uint256 newLiqFee, uint256 newRewardFee,
uint256 newMarketingFee, uint256 newDevFee, uint256 extraSellFee) external authorized {
    liquidityFee = newLiqFee;
    rewardsFee = newRewardFee;
    marketingFee = newMarketingFee;
    devFee = newDevFee;

    totalFee = liquidityFee.add(marketingFee).add(rewardsFee).add(devFee);

    totalFeeIfSelling = totalFee + extraSellFee;
    require(totalFeeIfSelling <= 25);
    emit feesChanged(totalFee, totalFeeIfSelling, liquidityFee, marketingFee, devFee, rewardsFee);
}

function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
    .....
    uint256 finalAmount = !isFeeExempt[sender] && !isFeeExempt[recipient] ? takeFee(sender, recipient, amount) : amount;
    _balances[recipient] = _balances[recipient].add(finalAmount);
    .....
}

function takeFee(address sender, address recipient, uint256 amount) internal returns (uint256) {
    uint256 feeApplicable = pair == recipient ? totalFeeIfSelling : totalFee;
    uint256 feeAmount = amount.mul(feeApplicable).div(100);

    _balances[address(this)] = _balances[address(this)].add(feeAmount);
    emit Transfer(sender, address(this), feeAmount);

    return amount.sub(feeAmount);
}
```

- **Recommendation:**
 - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.



THREAT LEVELS

. Informational

Owner can set max transaction limit, but cannot lower it than 0.5% of total supply.

```
function changeTxLimit(uint256 newLimit) external authorized {  
    require( newLimit >= 5, "Max tx cant be bellow 0.5%");  
    _maxTxAmount = newLimit.mul(_totalSupply).div(1000);  
    emit maxTxChanged(newLimit);  
}
```

Owner can exclude address from fees and transaction limits.

```
function changeIsFeeExempt(address holder, bool exempt) external authorized {  
    isFeeExempt[holder] = exempt;  
    emit feeExemptStatusChanged(holder, exempt);  
}  
  
function changeIsTxLimitExempt(address holder, bool exempt) external authorized {  
    isTxLimitExempt[holder] = exempt;  
    emit limitExemptStatusChanged(holder, exempt);  
}
```



Tokenomics:

There is no information about initial tokens distribution on the project's whitepaper and/or website.





Website

Website URL	https://babyshinja.co/
Domain Registry	https://ae.godaddy.com/
Domain Expiration	Expires on 2023-06-27
Technical SEO Test	Passed
Security Test	Passed. SSL certificate present

Design

- single page design appropriate color scheme and graphics

Whitepaper

- No whitepaper
- The information helps new investors understand what the product does right away. No grammar mistakes found..

Content

Roadmap

- Yes, goals set without time frames..

Mobile-friendly?.

- Yes

[Babyshinja.co](https://babyshinja.co/)



SOCIAL MEDIA& ONLINE PRESENCE

ANALYSIS

Project's social media pages are very active with activity from organic users



Twitter : @BabyShinja

- 2 331 Followers
- active
- Posts frequently



Telegram : @Baby_Shinja

- 195 members
- Active members
- Active mods



ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

RoyalProof

CRYPTO SECURITY

**Audits | KYCs | dApps
Contract Development**

FIND US ONLINE



<https://royalproof.net/>



@RoyalproofAudit



@RoyalProofOfficial



<https://github.com/Royal-Proof>



@RoyalProofAudit



@Royalproof_Admin



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency 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 Royal Proof and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Royal Proof) owe no duty of care towards you or any other person, nor does Royal Proof 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 Royal Proof 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, Royal Proof hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Royal Proof, 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, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.