Royalproof

Security Audit Report

Completed on

31,01,2023

OVERWIEW

This audit has been prepared for **SALAH** 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

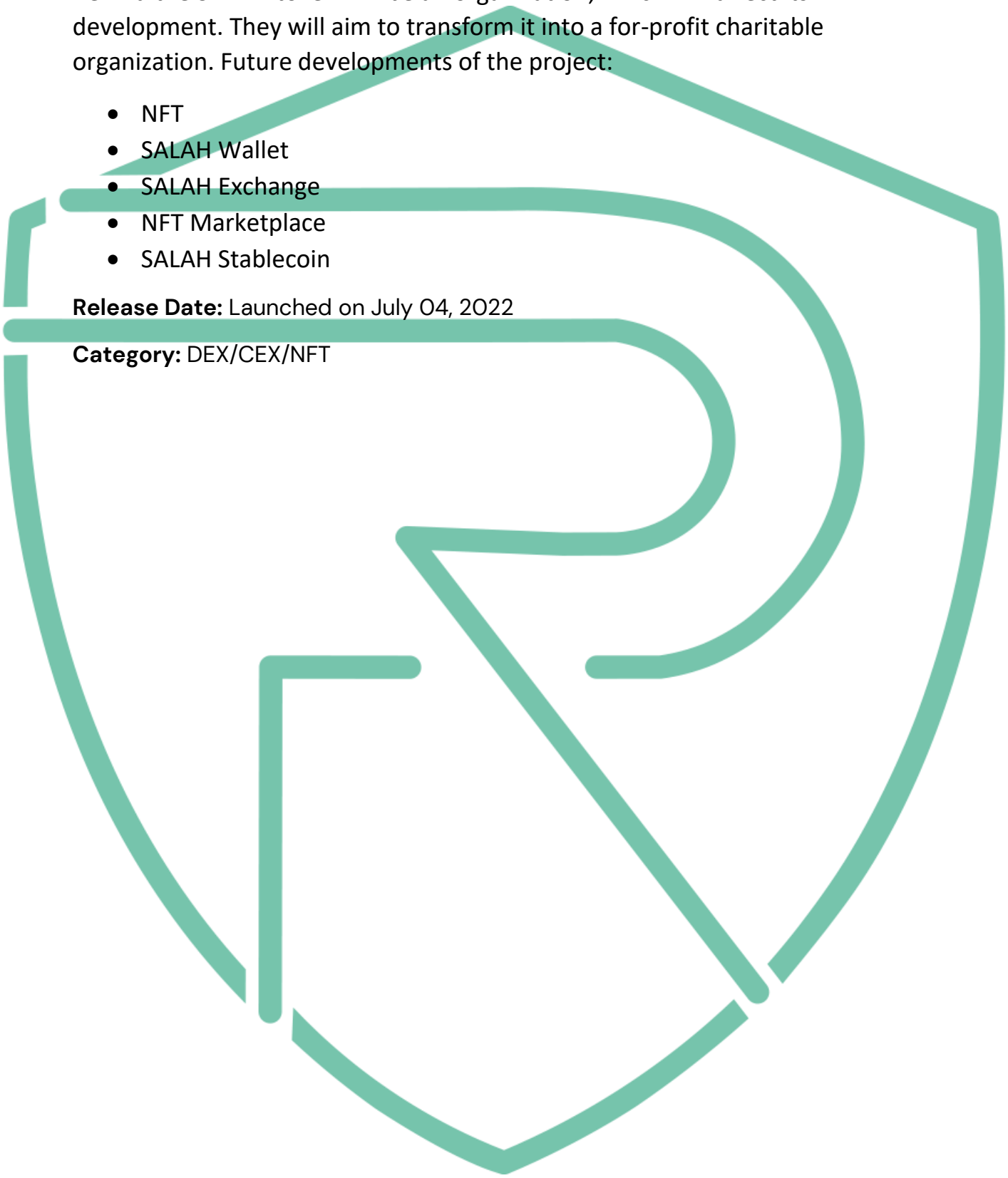
PROJECT DESCRIPTION

Behind the **SALAH** token will be an organization, which will direct its development. They will aim to transform it into a for-profit charitable organization. Future developments of the project:

- NFT
- SALAH Wallet
- SALAH Exchange
- NFT Marketplace
- SALAH Stablecoin

Release Date: Launched on July 04, 2022

Category: DEX/CEX/NFT



CONTRACT INFO

Token Name	Salah ad-Din
Symbol	SALAH
Contract Address	0x9F07C9112E482eb5e21d3c279d82203893e45CBa
Network	Binance Smart Chain
Language	Solidity
Deployment Date	26.06.2022
Verified?	Yes
Total Supply	1,000,000,000,000
Status	Launched

TAXES

Buy Tax	none
Sell Tax	none

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 July 07, 2022)

Status: Launched!

Liquidity: PancakeSwap: 55 WBNB

Burn: No tokens burnt

MaxTxAmount: No limit

DEX: PancakeSwap

LP Address(es): 0xD3A09F8e21De5213C375347525C679F9593FC42C

- **21% Unlocked 78.9% locked in PinkLock - unlocks at 2022.12.31**
  https://www.pinksale.finance/pinklock/record/1013950?chain=BSC

TOKEN TRANSFERS STATS

Transfer Count	1738
Uniq Senders	272
Uniq Receivers	381
Total Amount	5691980696918.518 SALAH
Median Transfer Amount	938065131.0501865 SALAH
Average Transfer Amount	3275017662.208583 SALAH
First transfer date	2022-06-26
Last transfer date	2022-07-06
Days token transferred	5

SMART CONTRACT STATS

Calls Count	5264
External calls	293
Internal calls	4971
Transactions count	2144
Uniq Callers	309
Days contract called	4
Last transaction time	2022-07-07 11:31:32 UTC
Created	2022-07-03 23:36:47 UTC
Create TX	0x8d893c5d053efcfa038dde352f9b51b64a4d7533a5a1037040c4a7e53dfe2ced
Creator	0xe53a02848392c8071636815a2d2adea58ded8ab4

FEATURED WALLETS

Owner address	0x30de33f6f557acd66e7919b9379044e2de4294b6
Dev Wallet	Same as owner
Charity Wallet	0x9eA8eA380eaEF925406231f37c8E6AEC729B5f06
Marketing wallet	0x1A51380dfE215971D375F67666504d4F4669c16B
LP address	**Pancakeswap:** 0xD3A09F8e21De5213C375347525C679F9593FC42C 21% Unlocked 78.9% locked in PinkLock - unlocks at 2022.12.31 https://www.pinksale.finance/pinklock/record/1013950?chain=BSC

*Address can be changed in future

TOP 3 UNLOCKED WALLETS

- 1- 0x1a039eb50948d95fe824ae7932cd79ca78d5f332 (6.85 %)
- 2- 0x0573f05a0fc193c5c6cca75e9324775cf90efb6e (3.60)
- 3- 0x4800a52c0b19d25e9b1e6db4bfee8929e6eb79b6 (2.94%)

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.

FOUND THREATS

- Medium Risk

  Owner can set buy/sell fees up to 20% (combined buy+sell = 40%).

```
uint256 public constant denominator = 10000;

function setBuyTax(uint256 _dev, uint256 _marketing,
 uint256 _liquidity, uint256 _charity) external onlyOwner {
    require(_dev <= 500,"SALAH: Maximum 5%");
    require(_marketing <= 500,"SALAH: Maximum 5%");
    require(_liquidity <= 500,"SALAH: Maximum 5%");
    require(_charity <= 500,"SALAH: Maximum 5%");

    buyTaxes["dev"] = _dev;
    buyTaxes["marketing"] = _marketing;
    buyTaxes["liquidity"] = _liquidity;
    buyTaxes["charity"] = _charity;
}

function setSellTax(uint256 _dev, uint256 _marketing,
 uint256 _liquidity, uint256 _charity) external onlyOwner {
    require(_dev <= 500,"SALAH: Maximum 5%");
    require(_marketing <= 500,"SALAH: Maximum 5%");
    require(_liquidity <= 500,"SALAH: Maximum 5%");
    require(_charity <= 500,"SALAH: Maximum 5%");

    buyTaxes["dev"] = _dev;
    buyTaxes["marketing"] = _marketing;
    buyTaxes["liquidity"] = _liquidity;
    buyTaxes["charity"] = _charity;
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined to to exceed 25%.

FOUND THREATS

- ## Medium Risk

  Owner can blacklist only contract addresses. If liquidity pair is blacklisted, this will lead to inability to trade.

```
function enableBlacklist(address account) external onlyOwner {
    require(isContract(account), "SALAH: Cannot blacklist users");
    require(!blacklist[account], "SALAH: Account is already blacklisted");
    blacklist[account] = true;
}
```

  - Recommendation:
    - Considered as good transfers limitation practice is liquidity pair to be excluded from such practices.

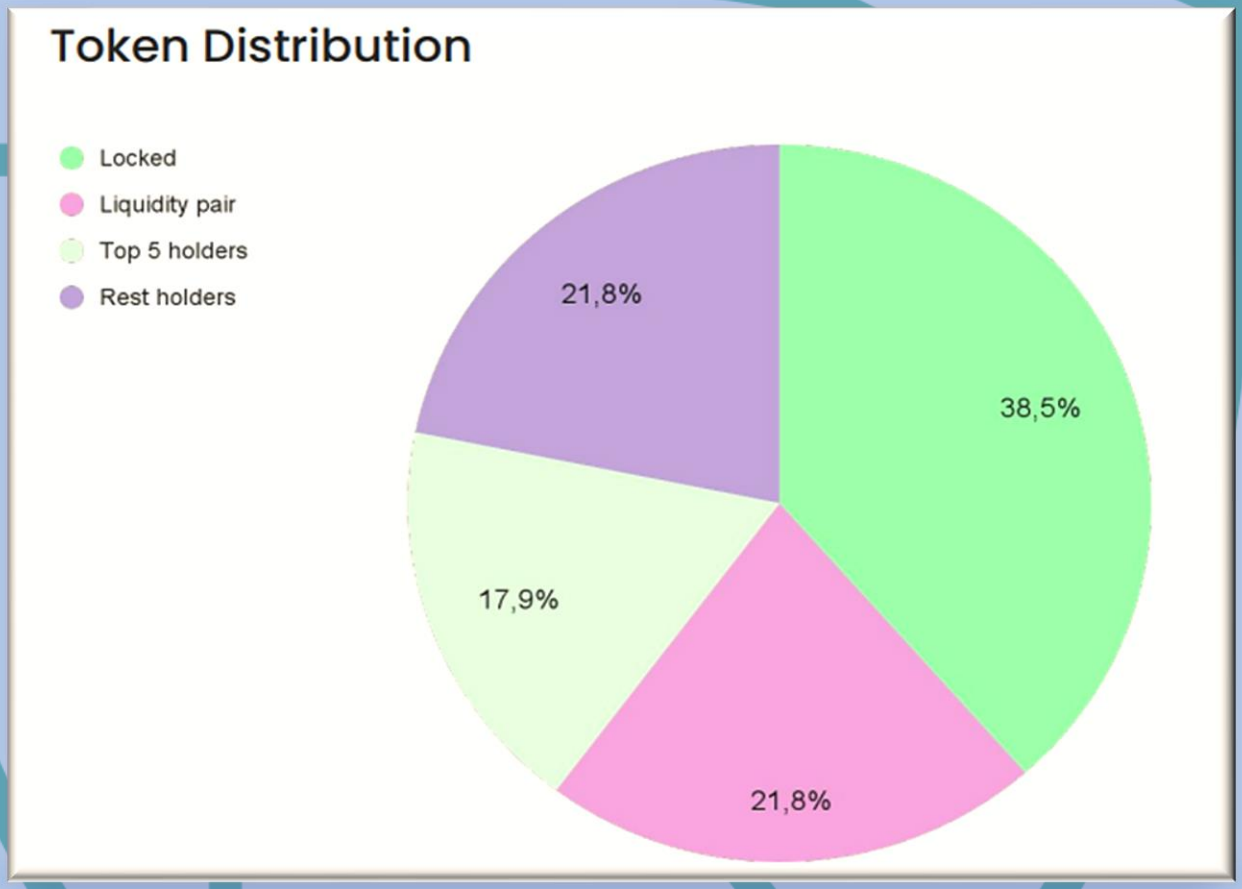
- ## Informational

  Owner can exclude address from taxes.

```
function exclude(address account) public onlyOwner {
    require(!isExcluded(account), "SALAH: Account is already excluded");
    excludeList[account] = true;
}
```

Tokenomics:

Locked in Pinklock	38,5%
Liquidity pair	21.76%
Top 5 holders	17.91%
Rest holders	21,83%



Website

Website URL
https://salah.finance/

Domain Registry
https://www.tucows.com/

Domain Expiration
Expires on 2023-04-11

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design

- single page design, appropriate color scheme, graphics and overall layout

Whitepaper

- Well written, explanatory.

Content

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

Roadmap

- Yes, goals set without time frames..

Mobile-friendly?.

- Yes

SOCIAL MEDIA& ONLINE PRESENCE

ANALYSIS

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

Twitter : @salahFinance

- 564Followers
- active
- Daily posts

Discord : @salahfinance

- 649 members
- few active memebers

Telegram : @SALAHFina

- 48 members
- Announcments channel
- few announcments each day

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.