InterFi NETWORK

SMART CONTRACT AUDIT

interfinetwork

hello@interfi.network

https://interfi.network

PREPARED FOR

LAIKA

INTRODUCTION

Auditing Firm	InterFi Network
Client Firm	Laika
Methodology	Automated Analysis, Manual Code Review
Contract	2hJBZzXhuX8XguKfQQCiwMC9jPfKpLtygYXEFZjAKR44
Blockchain	Solana
Metadata Source	QmU6eFw1rgk8QWAMdbH5RocXwgnxwCR6Ap8eztSDFvYB4F
Website	https://laikameme.top/
Telegram	https://t.me/laika_meme
X (Twitter)	https://x.com/laika__meme
Report Date	April 22, 2025

ℹ️ Verify the authenticity of this report on our website: https://www.github.com/interfinetwork

EXECUTIVE SUMMARY

InterFi has performed the automated and manual analysis of source codes. Source codes were reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical 🔴	Major 🟠	Medium 🟡	Minor 🟢	Unknown 🟤
Open	0	0	0	0	0
Acknowledged	0	0	0	1	0
Resolved	0	0	0	1	0

ℹ️ Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

ℹ️ Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on smart contract safety and security.

ℹ️ Please note that the absence of public KYC verification of the project owners, team members, or deployers associated with BioFi. Typically, third-party KYC processes are instrumental in ensuring the transparency and accountability of a project's leadership, thereby enhancing user trust and regulatory compliance.

TABLE OF CONTENTS

SCOPE OF WORK

InterFi was consulted by Laika to conduct the smart contract audit of their source codes. The audit scope of work is strictly limited to mentioned token only:

- 2hJBZzXhuX8XguKfQQCiwMC9jPfKpLtygYXEFZjAKR44

ℹ️ If source codes are not deployed on the main net, they can be modified or altered before main-net deployment. Verify the contract's deployment status below:

Token Link	
https://solscan.io/token/2hJBZzXhuX8XguKfQQCiwMC9jPfKpLtygYXEFZjAKR44#metadata	
Token Name	Laika
Owner Program	Token Program
Current Supply	1,000,000,000
Decimals	6
Token Extensions	False

AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of InterFi's auditing process and methodology:

CONNECT

- The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.

AUDIT

- Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:
  - Remix IDE Developer Tool
  - Open Zeppelin Code Analyzer
  - SWC Vulnerabilities Registry
  - DEX Dependencies, e.g., Pancakeswap, Uniswap
- Simulations are performed to identify centralized exploits causing contract and/or trade locks.
- A manual line-by-line analysis is performed to identify contract issues and centralized privileges. We may inspect below mentioned common contract vulnerabilities, and centralized exploits:

Centralized Exploits	○ Token Supply Manipulation ○ Access Control and Authorization ○ Assets Manipulation ○ Ownership Control ○ Liquidity Access ○ Stop and Pause Trading ○ Ownable Library Verification

Common Contract Vulnerabilities	○ Integer Overflow ○ Lack of Arbitrary limits ○ Incorrect Inheritance Order ○ Typographical Errors ○ Requirement Violation ○ Gas Optimization ○ Coding Style Violations ○ Re-entrancy ○ Third-Party Dependencies ○ Potential Sandwich Attacks ○ Irrelevant Codes ○ Divide before multiply ○ Conformance to Naming Guides ○ Compiler Specific Warnings ○ Language Specific Warnings

REPORT

- The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.
- The client's development team reviews the report and makes amendments to source codes.
- The auditing team provides the final comprehensive report with open and unresolved issues.

PUBLISH

- The client may use the audit report internally or disclose it publicly.

ℹ️ It is important to note that there is no pass or fail in the audit, it is recommended to view the audit as an unbiased assessment of the safety of source codes.

RISK CATEGORIES

Smart contracts are generally designed to hold, approve, and transfer tokens. This makes them very tempting attack targets. A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized here for the reader to review:

Risk Type	Definition
Critical 🔴	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major 🟠	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium 🟡	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor 🟢	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown 🟤	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.

CENTRALIZED PRIVILEGES

Centralization risk is the most common cause of cryptography asset loss. When a smart contract has a privileged role, the risk related to centralization is elevated.

There are some well-intended reasons have privileged roles, such as:

- Privileged roles can be granted the power to `pause()` the contract in case of an external attack.
- Privileged roles can use functions like, `include()`, and `exclude()` to add or remove wallets from fees, swap checks, and transaction limits. This is useful to run a presale and to list on an exchange.

Authorizing privileged roles to externally-owned-account (EOA) is dangerous. Lately, centralization-related losses are increasing in frequency and magnitude.

- The client can lower centralization-related risks by implementing below mentioned practices:
- Privileged role's private key must be carefully secured to avoid any potential hack.
- Privileged role should be shared by multi-signature (multi-sig) wallets.
- Authorized privilege can be locked in a contract, user voting, or community DAO can be introduced to unlock the privilege.
- Renouncing the contract ownership, and privileged roles.
- Remove functions with elevated centralization risk.

Understand the project's initial asset distribution. Assets in the liquidity pair should be locked. Assets outside the liquidity pair should be locked with a release schedule.

METADATA ANALYSIS

Metadata analysis in Solana blockchain involves scrutinizing the descriptive information that accompanies Solana tokens. This analysis delves into the data structure defined by "Metaplex protocol, focusing on attributes like the token's creator, mint authority, update authority, and associated multimedia files. By examining this metadata, we can assess token's compliance.

METAPLEX METADATA


```
{
key:
4
updateAuthority:
"4Wdn6wcbpWM61t96c7RpAaEbjSiEJ3jrtukqc5ZN3u65"
mint:
"2hJBZzXhuX8XguKfQQCiwMC9jPfKpLtygYXEFZjAKR44"
data:{4 items
name:
"LAIKA"
symbol:
"LAIKA"
uri:
"https://ipfs.io/ipfs/QmU6eFw1rgk8QWAMdbH5RocXwgnxwCR6Ap8eztSDFvYB4F"
sellerFeeBasisPoints:
0
}
primarySaleHappened:
0
isMutable:
0
editionNonce:
253
tokenStandard:
2
}
```

DEFINITION

Key	Definition
key	Identifies type of record in blockchain structure.
updateAuthority	Account authorized to update this metadata.
mint	Represents this token's creation account.
data	Object containing specific details about this token.
name	Name of this token.
symbol	Trading symbol of this token.
uri	Link to external information about this token, typically hosted on IPFS.
sellerFeeBasisPoints	Sales fee for this token, in basis points.
primarySaleHappened	Indicates whether this token has been sold for the first time.
isMutable	Specifies if metadata can be changed post-creation. Once changed to False, it cannot ever be True again
editionNonce	Optional field used for distinguishing editions of this token.
tokenStandard	Defines the compliance standard of this token.
description	Text description of this token, often including informative content.
Image	Link to an image of this token, usually stored on IPFS.

ANALYSIS

Key	Analysis
key	4
updateAuthority	4Wdn6wcbpWM61t96c7RpAaEbjSiEJ3jrtukqc5ZN3u65

mint	2hJBZzXhuX8XguKfQQCiwMC9jPfKpLtygYXEFZjAKR44
name	LAIKA
symbol	LAIKA
uri	https://ipfs.io/ipfs/QmU6eFw1rgk8QWAMdbH5RocXwgnxwCR6Ap8eztSDFvYB4F
sellerFeeBasisPoints	int0
primarySaleHappened	int0
isMutable	0
editionNonce	int253

KEY INFORMATION

Owner
4Wdn6wcbpWM61t96c7RpAaEbjSiEJ3jrtukqc5ZN3u65

CreateAccount transaction
56ry5pR9SLtZZWmV6WP4aeq3KLpkAi9LJLP1JLy2XYQFLSpb6NYWVsnoT1oMR1PpRhwyrVJcJxEDzMcpeaZAfQGi

totalSupply
1000000000

New mintTokens authority
NULL

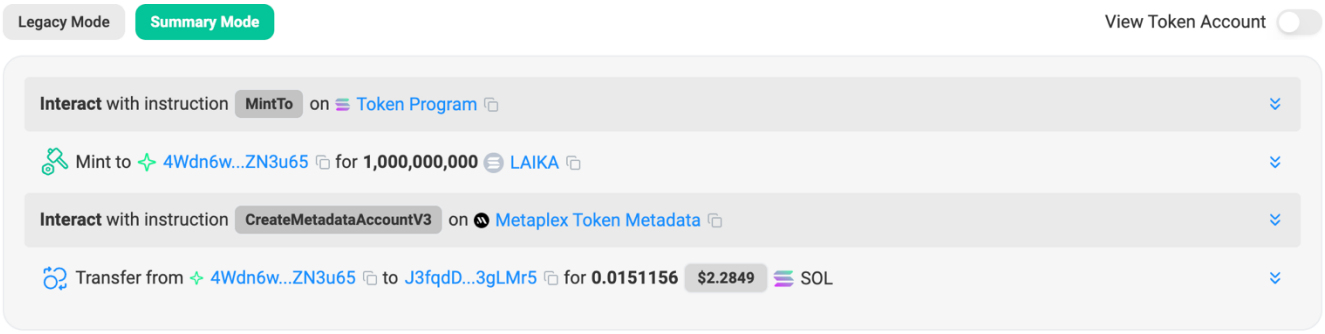
New `freezeAccount` authority
NULL

`isMutable`
0

MANUAL REVIEW

Identifier	Definition	Severity
CEN-02	Initial token distribution	Minor

Centralized role holds substantial portion of the circulating supply. Large number of tokens in one address raises significant concerns about centralization within the token's ecosystem.



RECOMMENDATION

Project must communicate with stakeholders and obtain the community consensus while distributing tokens.

RESOLUTION

Laika team argued that tokens are distributed as per their pre-determined tokenomics.

Identifier	Definition	Severity
CEN-03	Mint authority	NULL

Mint Authority is a designated account with the exclusive right to mint new tokens. This authority is used for controlling and manipulating the supply of the token. It enables controlled inflation or rewards distribution.

Mint authority is revoked:

https://solscan.io/tx/56ry5pR9SLtZZWmV6WP4aeq3KLpkAi9LJLP1JLy2XYQFLSpb6NYWVsnoT1oMR1PpRhwyrVJcJxEDzMcpeaZAfQGi

NOTE

No new `mintTokens` authority identified.

Identifier	Definition	Severity
CEN-04	Freeze authority	NULL

Freeze Authority is a designated account to halt or enable transactions for a specific token account, ensuring token compliance and security. It is similar to blacklist function, which allows specific accounts to be frozen, thus preventing transactions.

Freeze authority is revoked:

https://solscan.io/tx/56ry5pR9SLtZZWmV6WP4aeq3KLpkAi9LJLP1JLy2XYQFLSpb6NYWVsnoT1oMR1PpRhwyrVJcJxEDzMcpeaZAfQGi

NOTE

No new `freezeAccount` authority identified.

DISCLAIMERS

InterFi Network provides the easy-to-understand audit of blockchain source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other assets. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way

to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, INTERFI NETWORK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, INTERFI NETWORK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, INTERFI NETWORK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT'S OR ANY OTHER INDIVIDUAL'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. InterFi Network does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.

LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than InterFi Network. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites' and social accounts' owners. You agree that InterFi Network is not responsible for the content or operation of such websites and social accounts and that InterFi Network shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.

ABOUT INTERFI NETWORK

InterFi Network provides intelligent blockchain solutions. We provide smart contract development, testing, and auditing services. We have developed 150+ solidity codes, audited 1000+ smart contracts, and analyzed 500,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Velas, Oasis, etc.

InterFi Network is built by engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 4 core members, and 6+ casual contributors.

Website: https://interfi.network

Email: hello@interfi.network

GitHub: https://github.com/interfinetwork

Telegram (Engineering): https://t.me/interfiaudits

Telegram (Onboarding): https://t.me/interfisupport

interfinetwork

hello@interfi.network

https://interfi.network

SMART CONTRACT AUDITS | SOLIDITY DEVELOPMENT AND TESTING

RELENTLESSLY SECURING PUBLIC AND PRIVATE BLOCKCHAINS