





SMART CONTRACT AUDIT | SOLIDITY DEVELOPMENT & TESTING | KYC | PROJECT EVALUATION

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN

Summary

Auditing Firm InterFi Network

Client Firm Melodity

Architecture InterFi "Echelon" Auditing Standard

Platform Solidity

Mandatory Audit Check Static, Software, Auto Intelligent & Manual Analysis

Final Report Date December 06, 2021

<u>Audit Summary</u>

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

- Melodity's private sale smart contract source code has LOW RISK SEVERITY
- The smart contract has PASSED the audit

For the detailed understanding of risk severity, source code vulnerability, and functional test, kindly refer to the audit.

✓ Verify the authenticity of this report on InterFi's GitHub: https://github.com/interfinetwork



Table Of Contents

<u>Project Information</u>

Overview	4
InterFi "Echelon" Audit Standard	
Audit Scope & Methodology	6
InterFi's Risk Classification	8
Smart Contract Risk Assessment	
Static Analysis	9
Software Analysis	10
Manual Analysis	12
SWC Attacks	16
Risk Status & Radar Chart	18
Report Summary	
Auditor's Verdict	19
<u>Legal Advisory</u>	
Important Disclaimer	20
About InterFi Network	21



Project Overview

InterFi was consulted by Melodity to conduct the smart contract security audit of the private sale's solidity source code.

About Melodity

Melodity™ token (ticker \$MELD) is a DeFi token hosted on the Binance Smart Chain (BSC). It is the store of value for the environment acting as a share token. The project aims to redistribute power from intermediaries and middlemen that formed in the early days of recorded music to musicians, enabling artists to distribute their creations on their own. Melodity was founded in 2021, and the MELD token is designed to change how independent musicians earn revenue from their creations giving them the freedom to monetize while increasing their visibility in the musical scene. Melodity Protocol will be expanding to empower the Do Ecosystem that includes: a Proprietary Blockchain, Tokens, Dapps, NFT marketplaces and NGOs which will allow musicians to distribute their own music. Melodity protocol has an ambitious roadmap thanks to its growing popularity and they wish to be listed on the leading exchanges, and increase their partnerships.

Project	Melodity
Blockchain	Binance Smart Chain
Language	Solidity
Contract	Not Deployed
Website	https://melodity.org/
Instagram	https://instagram.com/melodityofficial
Medium	https://medium.com/@melodityofficial



Project Logo



Solidity Source Code On InterFi GitHub

https://github.com/interfinetwork/audited-codes/blob/main/MelodityPS.sol

SHA-1 Hash

Solidity source code is audited at hash #c31fe6921a6d28e0f4f2be9bc40094187967989f



Audit Scope & Methodology

The scope of this report is to audit the smart contract source code of Melodity's Private Sale. InterFi has scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category

- Re-entrancy
- Unhandled Exceptions
- Transaction Order Dependency
- Integer Overflow
- Unrestricted Action
- Incorrect Inheritance Order
- Typographical Errors
- Requirement Violation
- Ownership Takeover
- Gas Limit and Loops
- Deployment Consistency
- Repository Consistency
- Data Consistency
- Token Supply Manipulation
- Access Control and Authorization
- Operations Trail and Event Generation
- Assets Manipulation
- Liquidity Access

Smart Contract Vulnerabilities

Source Code Review

Functional Assessment



InterFi's Echelon Audit Standard

The aim of InterFi's "Echelon" standard is to analyze the smart contract and identify the vulnerabilities and the hacks in the smart contract. Mentioned are the steps used by ECHELON-1 to assess the smart contract:

- 1. Solidity smart contract source code reviewal:
 - Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, scope, and functionality of the smart contract.
 - Manual review of code, which is the process of reading source code line-byline to identify potential vulnerabilities.
- 2. Static, Manual, and Software analysis:
 - Test coverage analysis, which is the process of determining whether the test cases are covering the code and how much code is exercised when we run those test cases.
 - Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
- 3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
- 4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts

Automated 3P frameworks used to assess the smart contract vulnerabilities

- Slither
- Consensys MythX, Mythril
- SWC Registry
- Solidity Coverage
- Open Zeppelin Code Analyzer
- Solidity Code Complier



InterFi's Risk Classification

Smart contracts are generally designed to manipulate and hold funds denominated in ETH/BNB. This makes them very tempting attack targets, as a successful attack may allow the attacker to directly steal funds from the contract. Below are the typical risk levels of a smart contract:

Vulnerable: A contract is vulnerable if it has been flagged by a static analysis tool as such. As we will see later, this means that some contracts may be vulnerable because of a false-positive.

Exploitable: A contract is exploitable if it is vulnerable and the vulnerability could be exploited by an external attacker. For example, if the "vulnerability" flagged by a tool is in a function which requires to own the contract, it would be vulnerable but not exploitable.

Exploited: A contract is exploited if it received a transaction on the main network which triggered one of its vulnerabilities. Therefore, a contract can be vulnerable or even exploitable without having been exploited.

-• •		SHIGH CONTINCT
Risk severity	Meaning	Security Audit
! Critical	This level vulner	abilities could be exploited easily, and can lead to asset loss, data
	loss, asset mani	pulation, or data manipulation. They should be fixed right away.
! High	This level vulner	rabilities are hard to exploit but very important to fix, they carry an
	elevated risk of	smart contract manipulation, which can lead to critical risk severity
! Medium	This level vulner	abilities are should be fixed, as they carry an inherent risk of future
	exploits, and ha	cks which may or may not impact the smart contract execution.
	This level vulne	erabilities can be ignored. They are code style violations, and
! Low	informational s	tatements in the code. They may not affect the smart contract
	execution	



Smart Contract - Static Analysis

Symbol Meaning Function can be modified Function is payable S Function is locked Function can be accessed Important functionality | **<mark>IMelodity</mark>** | Interface | ||| | └ | insertLock | External ! | ● |NO! | | L | decimals | External ! | P | NO! | | L | release | External ! | • |NO! | | L | burn | External ! | • |NO! | | L | balanceOf | External ! | O | NO! | | **PrivateSale** | Implementation | Ownable ||| | └ | <Constructor> | Public ! | ● |NO! | | L | getLatestPrice | Public ! | NO! | | L | <Receive Ether> | External ! | MO! | | L | getReferral | Private 🔐 | | | | L | addReferral | Public ! | 🔎 | onlyOwner | | L | buy | Public ! | 💹 |NO! | | L | release | Public ! | 🔎 | onlyOwner | | L | updateMaxRelease | Public ! | | onlyOwner | | └ | <mark>burnUnsold</mark> | Public ! | ● | onlyOwner | | L | createSelfLock | Public ! | • | onlyOwner | | L | releasedManualOverride | Public ! | Public ! | onlyOwner |

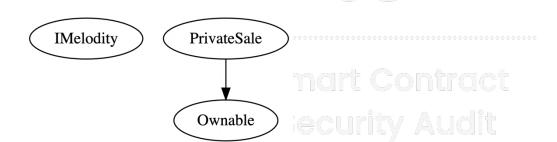


Smart Contract - Software Analysis

Function Signatures

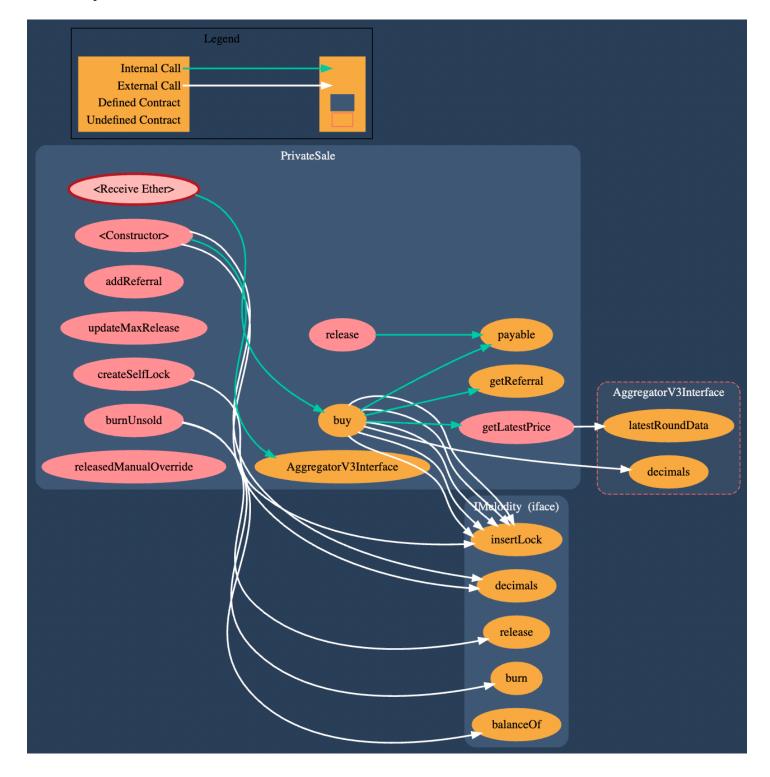
```
ae026bd3 => insertLock(address,uint256,uint256)
             decimals()
313ce567 =>
37bdc99b =>
             release(uint256)
42966c68 => burn(uint256)
70a08231 => balanceOf(address)
8e15f473 => getLatestPrice()
a749df4b => getReferral(string)
ec90d8d4 =>
             addReferral(string,uint256,uint8,uint256,uint256)
492cc769 \Rightarrow buy(string)
86d1a69f => release()
6f2e05a1 => updateMaxRelease(uint256)
b52a5851 => burnUnsold()
d9771aa9 => createSelfLock()
e2d276a2 => releasedManualOverride(uint256)
```

Inheritance Graph





<u>Call Graph</u>





Smart Contract – Manual Analysis

Function	Description	Tested	Verdict
Total Supply	provides information about the total token	NA	NA
rotal supply	supply		
Balance Of	provides account balance of the owner's	Yes	Passed
buluiice Oi	account		
Transfer	executes transfers of a specified number of	NA	NA
Transier	tokens to a specified address		
Ammento	allow a spender to withdraw a set number of		Passed
Approve	tokens from a specified account	Yes	
Allowance	returns a set number of tokens from a spender to		NA
Allowance	the owner	NA	
	is an action in which the project buys back its		
Buy Back	tokens from the existing holders usually at a	NA	NA
	market price all Contract		
Purp	executes transfers of a specified number of	Yes	Passed
Burn	tokens to a burn address		
Mint	executes creation of a specified number of		
MIIIC	tokens and adds it to the total supply	NA	NA
	circulating token supply adjusts (increases or		
Rebase	decreases) automatically according to a token's	NA	NA
	price fluctuations		
Blacklist	stops specified wallets from interacting with the		
BIGCKIISC	smart contract function modules	NA	NA
Lock	locks all tokens for a specified time period	Yes	Passed



Function	Description	Tested	Verdict
Dividend	executes transfers of a specified dividend token to a specified address	NA	NA
Airdrop	executes transfers of a specified number of tokens to a specified address	NA	NA
Max Transaction	a non-whitelisted wallet can only transfer a specified number of tokens	NA	NA
Max Wallet	a non-whitelisted wallet can only hold a specified number of tokens	NA	NA
Anti Bot	stops some or all bot wallets from interacting with the smart contract	NA	NA
Transfer Ownership	executes transfer of contract ownership to a specified wallet	NA	NA
Renounce Ownership	executes transfer of contract ownership to a dead address	NA	NA





- Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.
- Smart contract owner locks partial tokens and releases them on a strict schedule.

Smart contract collects the funds and sends it to the mentioned multi-sig wallet.

```
/**
  * Release the funds on this smart contract to the multisig wallet
  */
function release() public onlyOwner {
    // company wallet: 0x01Af10f1343C05855955418bb99302A6CF71aCB8
    uint256 balance = address(this).balance;
    payable(0x01Af10f1343C05855955418bb99302A6CF71aCB8).transfer(balance);
    emit Released(balance);
}
```

A manual override is allowed to release the private sale tokens.

```
/**
 * Allow for the release of private sale manually, the provided amount was manually
 * released in other ways and is added to the already released amount
 */
function releasedManualOverride(uint256 additionalAmount) public onlyOwner {
    released += additionalAmount;
}
```



}

The smart contract has low severity issue which may or may not create any functional vulnerability.

```
"resource": "/Melodity.sol",

"owner": "_generated_diagnostic_collection_name_#0",

"severity": 8, (! Low Severity)

"Expected identifier, got 'LParen",

"source": "solc",
}
```

Smart Contract Security Audit



Smart Contract - SWC Attacks

SWC ID	Description	Verdict
SWC-101	Integer Overflow and Underflow	! Low
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
swc-107	Re-entrancy	Passed
swc-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation Smart Contract	Passed
swc-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegate Call to Untrusted Callee	Passed
swc-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-116	Block values as a proxy for time	Passed
swc-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed

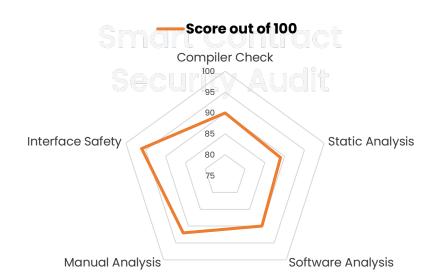


SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects (Irrelevant/Dead Code)	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed



Smart Contract - Risk Status & Radar Chart

Risk Severity	Status
! Critical	None critical severity issues identified
! High	None high severity issues identified
! Medium	None medium severity issues identified
! Low	1 low severity issue identified
Verified	54 functions and instances verified and checked
Safety Score	96 out of 100





Auditor's Verdict

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks.

Melodity's private sale smart contract source code has LOW RISK SEVERITY.



Note for stakeholders

- Be aware that active smart contract owner privileges constitute an elevated impact on smart contract's safety and security.
- ❖ Make sure that the project team's KYC/identity is verified by an independent firm, e.g., InterFi.
- Always check if the contract's liquidity is locked. A longer liquidity lock plays an important role in project's longevity. It is recommended to have multiple liquidity providers.
- Examine the unlocked token supply in the owner, developer, or team's private wallets. Understand the project's tokenomics, and make sure the tokens outside of the LP Pair are vested or locked for a longer period of time.
- Ensure that the project's official website is hosted on a trusted platform, and is using an active SSL certificate. The website's domain should be registered for a longer period of time.



Important Disclaimer

InterFi Network provides contract auditing and project verification services for blockchain projects. The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project. This report should not be transmitted, disclosed, referred to, or relied upon by any person for any purposes without InterFi's prior written consent.

InterFi provides the easy-to-understand assessment of the project, and the smart contract (otherwise known as the source code). The audit makes no statements or warranties on the security of the code. It also cannot be considered as an enough assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have used all the data at our disposal to provide the transparent analysis, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Be aware that smart contracts deployed on a blockchain aren't resistant from external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security. Therefore, InterFi does not guarantee the explicit security of the audited smart contract.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

This report should not be considered as an endorsement or disapproval of any project or team.

The information provided on 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. Do conduct your own due diligence and consult your financial advisor before making any investment decisions.



About InterFi Network

InterFi Network provides intelligent blockchain solutions. InterFi is developing an ecosystem that is seamless and responsive. Some of our services: Blockchain Security, Token Launchpad, NFT Marketplace, etc. InterFi's mission is to interconnect multiple services like Blockchain Security, DeFi, Gaming, and Marketplace under one ecosystem that is seamless, multi-chain compatible, scalable, secure, fast, responsive, and easy-to-use.

InterFi is built by a decentralized team of UI experts, contributors, engineers, and enthusiasts from all over the world. Our team currently consists of 6+ core team members, and 10+ casual contributors. InterFi provides manual, static, and automatic smart contract analysis, to ensure that project is checked against known attacks and potential vulnerabilities.

To learn more, visit https://interfi.network

To view our audit portfolio, visit https://github.com/interfinetwork

To book an audit, message https://t.me/interfiaudits



