VITAL BLOCK

Security Assessment

SUIHEROES

Vital Block Verified on July 31ST, 2023

@Vital-Block

@VB_Audit

info@vitalblock.org

www.vitalblock.org

PREPARED FOR:

SUIHEROES

INTRODUCTION

Auditing Firm	**VITAL BLOCK SECURITY**
Client Firm	**SUIHEROES**
Methodology	Automated Analysis, Manual Code Review
Language	Move
Contract Address	0xca7ba1c8700a67145c4b700c900cb9bb137ef2e2a9e59db63b7a71136c57ab4b
Source Code Light	**Verified**
Code File	**Coinflip.Move**
Centralization	Active ownership
Compiler Version	**v0.8.18+commit.87f61d96**
Blockchain	**SUI NETWORK**
Website	**https://suiheroes.com/coinflip**
Discord	**https://discord.com/invite/7p69hGAFwg**
Twitter	**https://twitter.com/Suiheroes_io**
Doc	**https://medium.com/@suiheroes**
Prelim Report Date	August 1st 2023
Final Report Date	August 1st 2023

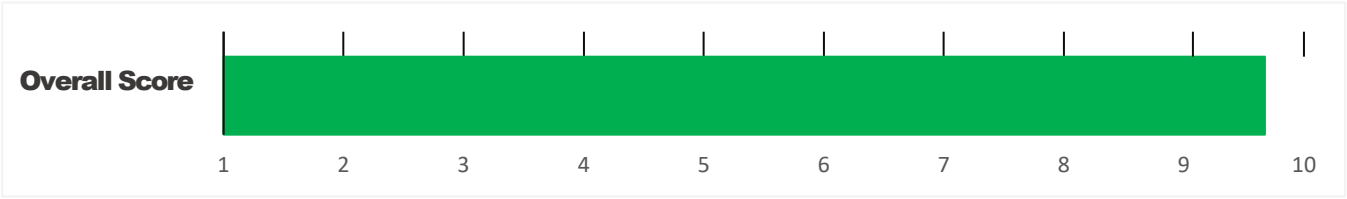
Verify the authenticity of this report on our GitHub Repo: https://www.github.com/vital-block

EXECUTIVE SUMMARY

Vital Block Security has performed the automated and manual analysis of the COINFLIP Move code. The code was reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical ! 🔴	Major " 🟠	Medium # 🟡	Minor $ 🟢	Unknown % 🟤
Open	0	0	1	3	0
Acknowledged	0	0	1	2	0
Resolved	0	0	0	0	0
Noteworty onlyOwner Privileges	Set Taxes and Ratios, Airdrop, Set Protection Settings, Set Reward Properties, Set Reflector Settings, Set Swap Settings, Set Pair and Router				

COINFLIP Smart contract has achieved the following score: 97.0



ⓘ **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.**

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

TABLE OF CONTENTS

SCOPE OF WORK

Vital Block was consulted by SUIHEROES to conduct the smart contract audit of its. Move source code. The audit scope of work is strictly limited to mentioned .Sol file only:

O.SUIHEROES.sol

External contracts and/or interfaces dependencies are not checked due to being out of scope.

Verify audited contract's contract address and deployed link below:

Public Contract Address	
https://suiscan.xyz/mainnet/object/0xca7ba1c8700a67145c4b700c900cb9bb137ef2e2a9e59cb63b7a71136c57ab4b	
Contract Name	**Coinflip.move**
Package	**Suiheroes Coinflip**

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 Vital Block Security 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 Solidity 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 the 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.

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 solidity 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.

AUTOMATED ANALYSIS

Symbol	Definition
🛑	**Function modifies state**
💷	**Function is payable**
🔒	**Function is internal**
🔐	**Function is private**
❗	**Function is important**

COINFLIP	Interface			
└	totalSupply	External		❗	NO
└	decimals	External		❗	NO
└	symbol	External		❗	NO
└	name	External		❗	NO
└	getOwner	External			NO
└	balanceOf	External		❗	NO
└	transfer	External	"	❗	🛑	NO
└	allowance	External		❗	NO
└	approve	External	"	❗	🛑	NO
└	transferFrom	External	"		NO

IFactoryV2	Interface			
└	getPair	External			NO
└	createPair	External	"		NO

IV2Pair	Interface			
└	factory	External			NO
└	getReserves	External			NO
└	sync	External	"		NO

IRouter01	Interface			
└	factory	External ❗	|NO❗
└	Sol	External ❗		NO❗
└	addLiquiditySUI	External ❗	#	NO❗
└	addLiquidity	External ❗	" |NO❗
└	swapExactETorTokens	External ❗	# |NO❗
└	getAmountsOut	External ❗	|NO❗
└	getAmountsIn	External ❗	|NO❗
IRouter02	Interface	IRouter01		
└	swapExactTokensForSUISupportingFeeOnTransferTokens	External ❗	" |NO❗
└	swapExactSUIForTokensSupportingFeeOnTransferTokens	External ❗	# |NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	" ! 🛑 |NO❗
└	swapExactTokensForTokens	External ❗	" |NO❗
Protections	Interface			
└	checkUser	External ❗	" ! 🛑 |NO❗
└	setLaunch	External ❗	" |NO❗
└	setLpPair	External ❗	" |NO❗
└	SUI	External ❗	" |NO❗
└	removeSniper	External ❗	" |NO❗
Cashier	Interface			
└	setRewardsProperties	External ❗	" |NO❗
└	tally	External ❗	" |NO❗
└	load	External ❗	# |NO❗
└	cashout	External ❗	" |NO❗
└	giveMeWelfarePlease	External ❗	" |NO❗
└	getTotalDistributed	External ❗	|NO❗
└	getUserInfo	External ❗	|NO❗
└	getUserRealizedRewards	External ❗	|NO❗

| └ | getPendingRewards | External ❗ | | NO❗ |

| └ | initialize | External ❗ | " | NO❗ |

| └ | getCurrentReward | External ❗ | | NO❗ |

||||||

| **MOVE** | Implementation | **SafeMath** |||

| └ | <Constructor> | Public ❗ | | # | NO❗ |

| └ | transferOwner | External ❗ | " | onlyOwner |

| └ | renounceOwnership | External ❗ | " | NO❗ |

| └ | setOperator | Public ❗ | " | NO❗ |

| └ | renounceOriginalDeployer | External ❗ | " | NO❗ |

| └ | <Receive SUI> | External ❗ | | # | NO❗ |

| └ | totalSupply | External ❗ | | NO❗ |

| └ | decimals | External ❗ | | NO❗ |

| └ | symbol | External ❗ | | NO❗ |

| └ | name | External ❗ | | NO❗ |

| └ | getOwner | External ❗ | | ❗ | NO❗ |

| └ | balanceOf | Public ❗ | | ❗ | NO❗ |

| └ | allowance | External ❗ | | ❗ | NO❗ |

| └ | approve | External ❗ | " | ❗ 🛑 | NO❗ |

| └ | _approve | Internal $ | " 🔒 🛑 | |

| └ | approveContractContingency | Public ❗ | " | ❗ 🛑 | onlyOwner |

| └ | transfer | External ❗ | " | NO❗ |

| └ | transferFrom | External ❗ | " | NO❗ |

| └ | setNewRouter | External ❗ | " | onlyOwner |

| └ | setLpPair | External ❗ | " | onlyOwner |

| └ | setInitializers | External ❗ | " | onlyOwner |

| └ | isExcludedFromFees | External ❗ | | NO❗ |

| └ | isExcludedFromDividends | External ❗ | | NO❗ |

| └ | isExcludedFromProtection | External ❗ | | NO❗ |

| └ | setDividendExcluded | Public ❗ | " | onlyOwner |

| └ | setExcludedFromFees | Public ❗ | " | onlyOwner |

BTV-01 POSSIBLE OVERFLOW

Category	Severity	Location	Status
Suboptimal	**Minor**	Contract/Coinflip.move	Acknowledged

Description

In **GamePool ,** the following equation is used inside an unchecked block

```
entry withdraw<Ty0: drop>(Arg0: &mut GamePool<Ty0>, Arg1: u64, Arg2: &mut TxContext) {
B0:
    0: CopyLoc[2](Arg2: &mut TxContext)
    1: FreezeRef
    2: Call tx_context::sender(&TxContext): address
    3: CopyLoc[0](Arg0: &mut GamePool<Ty0>)
    4: ImmBorrowFieldGeneric[0](GamePool.owner: address)
    5: ReadRef
```

Where parameters. Block **GamePool** Out Used is a this and override In is a this.
As these two are multiplied together in an unchecked block, they may overflow.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the PairsIn is close enough it will never causean overflow

BST-02 POSSIBLE OVERFLOW

Category	Severity	Location	Status
Status Mathematical Operations	**Minor**	Contract/Coinflip.move	Acknowledged

Description

In **PalyerData ,** the following equation is used inside an unchecked block

```
CopyLoc[8](loc2: &mut PlayerData)
   88: MutBorrowField[6](PlayerData.amount: u64)
   89: WriteRef
   90: CopyLoc[3](Arg3: u8)
   91: CopyLoc[8](loc2: &mut PlayerData)
   92: MutBorrowField[7](PlayerData.select: u8)
   93: WriteRef
```

Recommendation

We recommend either checking for overflow in this case, or ensuring that the PairsIn is close enough it will never cause an overflow.

FZT-03 POSSIBLE OVERFLOW

Category	Severity	Location	Status
Inconsistency	**Informational**	Contract/Coinflip.move	Acknowledged

Description

In **updateForBalance** , the following equation is used inside an unchecked block

```
 46: MutBorrowFieldGeneric[3](GamePool.balance: Balance<Ty0>)
47: MoveLoc[1](Arg1: Coin<Ty0>)
48: Call coin::into_balance<Ty0>(Coin<Ty0>): Balance<Ty0>
49: Call balance::join<Ty0>(&mut Balance<Ty0>, Balance<Ty0>): u64
```

The function Balance () does not have the override specifier. It should be noted that since price0 > a function that overrides only a single interface function does not require the override specifier (see doc). However, all other instances of this in the code base contain the override specifier.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the PairsIn is close enough it will never cause an overflow.

OPTIMIZATIONS | COINFLIP

ID	Title	Category	Status
FTV	Logarithm Refinement Optimization	Gas Optimization	Acknowledged
FOP	Checks Can Be Performed Earlier	Gas Optimization	Acknowledged
FDP	Unnecessary Use Of SafeMath	Gas Optimization	Acknowledged
FWY	Struct Optimization	Gas Optimization	Acknowledged
FGT	Unused State Variable	Gas Optimization	Acknowledged

General Detectors

Missing Zero Address Validation

Some functions in this contract may not appropriately check for zero addresses being used.

Attention Required

Incorrect Solidity Version

This contract uses an unconventional or very old version of Solidity

Attention Required

- No compiler version inconsistencies found
- No unchecked call responses found
- No vulnerable self-destruct functions found
- No assertion vulnerabilities found
- No old solidity code found
- No external delegated calls found
- No external call dependency found
- No vulnerable authentication calls found
- No invalid character typos found
- No RTL characters found
- No dead code found
- No risky data allocation found
- No uninitialized state variables found
- No uninitialized storage variables found
- No vulnerable initialization functions found
- No risky data handling found
- No number accuracy bug found
- No out-of-range number vulnerability found
- No map data deletion vulnerabilities found
- No tautologies or contradictions found
- No faulty true/false values found
- No innacurate divisions found
- No redundant constructor calls found
- No vulnerable transfers found
- No vulnerable return values found
- No uninitialized local variables found
- No default function responses found
- No missing arithmetic events found
- No missing access control events found
- No redundant true/false comparisons found
- No state variables vulnerable through function calls found
- No buggy low-level calls found
- No expensive loops found
- No bad numeric notation practices found
- No missing constant declarations found
- No missing external function declarations found
- No vulnerable payable functions found
- No vulnerable message values found

Vulnerability Scan

REENTRANCY

No reentrancy risk found

Severity	Minor
Confidence Parameter	Certain

Vulnerability Description

Not Mintable: A large amount of this token can not be minted by a private wallet or contract.

Scanning Line:

```
entry live_game<Ty0: drop>(Arg0: &mut GamePool<Ty0>,
Arg1: bool, Arg2: &mut TxContext) {
B0:
    0: MoveLoc[2](Arg2: &mut TxContext)
    1: FreezeRef
    2: Call tx_context::sender(&TxContext): address
    3: CopyLoc[0](Arg0: &mut GamePool<Ty0>)
    4: ImmBorrowFieldGeneric[0](GamePool.owner: address)
    5: ReadRef
    6: Eq
    7: BrFalse(9)
B1:
    8: Branch(13)
B2:
    9: MoveLoc[0](Arg0: &mut GamePool<Ty0>)
    10: Pop
    11: LdConst[3](U64: 04000000..)
    12: Abort
```

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor

```
13: MoveLoc[1](Arg1: u16)
    14: MoveLoc[0](Arg0: &mut GamePool<Ty0>)
    15: MutBorrowFieldGeneric[1](GamePool.fee: u16)
    16: WriteRef
    17: Ret
```

Description:

Floating point calculations can vary across different architectures.

Alleviation:

This exhibit was acknowledged and ultimately discarded by the **SUIHEROES** team due to low severity. We consider the exhibit fully attended to as it doesn't impose any meaningful security concerns.

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.

Contract Owner Address:

0x1b2afab3bb2ee1f837a8dd7ab13ff8d2c77f446d0dc80ce8b43fb4c9c213b8bc

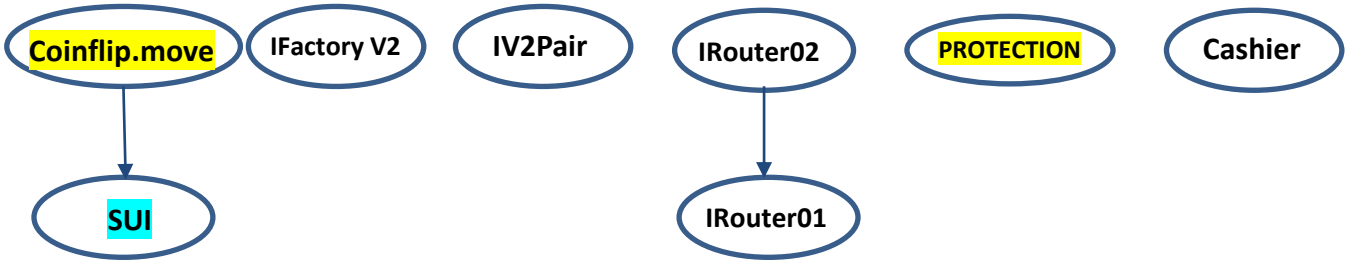
Audited Files

Coinflip.move

Contracts:

Contract :
Coinflip::0xca7ba1c8700a67145c4b700c900cb9bb137ef2e2a9e59cb63b7a71136c57ab4b

INHERITANCE GRAPH



Identifier	Definition	Severity
CEN-12	Centralization privileges of COINFLIP	Medium # 🟡

Vulnerability 0 : No important security issue detected.
Threat level: Low

Home | Coinflip.move

```
    13: LdConst[3](U64: 04000000..)
    14: Abort
B3:
    15: MoveLoc[0](Arg0: &mut GamePool<Ty0>)
    16: MutBorrowFieldGeneric[3](GamePool.balance: Balance<Ty0>)
    17: MoveLoc[1](Arg1: u64)
    18: Call balance::split<Ty0>(&mut Balance<Ty0>, u64): Balance<Ty0>
    19: CopyLoc[2](Arg2: &mut TxContext)
    20: Call coin::from_balance<Ty0>(Balance<Ty0>, &mut TxContext): Coin<Ty0>
    21: MoveLoc[2](Arg2: &mut TxContext)
    22: FreezeRef
    23: Call tx_context::sender(&TxContext): address
    24: Call transfer::public_transfer<Coin<Ty0>>(Coin<Ty0>, address)
    25: Ret
}
entry play<Ty0: drop>(Arg0: &mut GamePool<Ty0>, Arg1: Coin<Ty0>, Arg2: u64, Arg3: u8, Arg4: &Clock, Arg5: &mut TxContext) {
B0:
    0: CopyLoc[2](Arg2: u64)
    1: CopyLoc[2](Arg2: u64)
    2: CopyLoc[0](Arg0: &mut GamePool<Ty0>)
    3: ImmBorrowFieldGeneric[1](GamePool.fee: u16)
    4: ReadRef
    5: CastU64
    6: Mul
    7: LdU64(10000)
    8: Div
```

MANUAL REVIEW

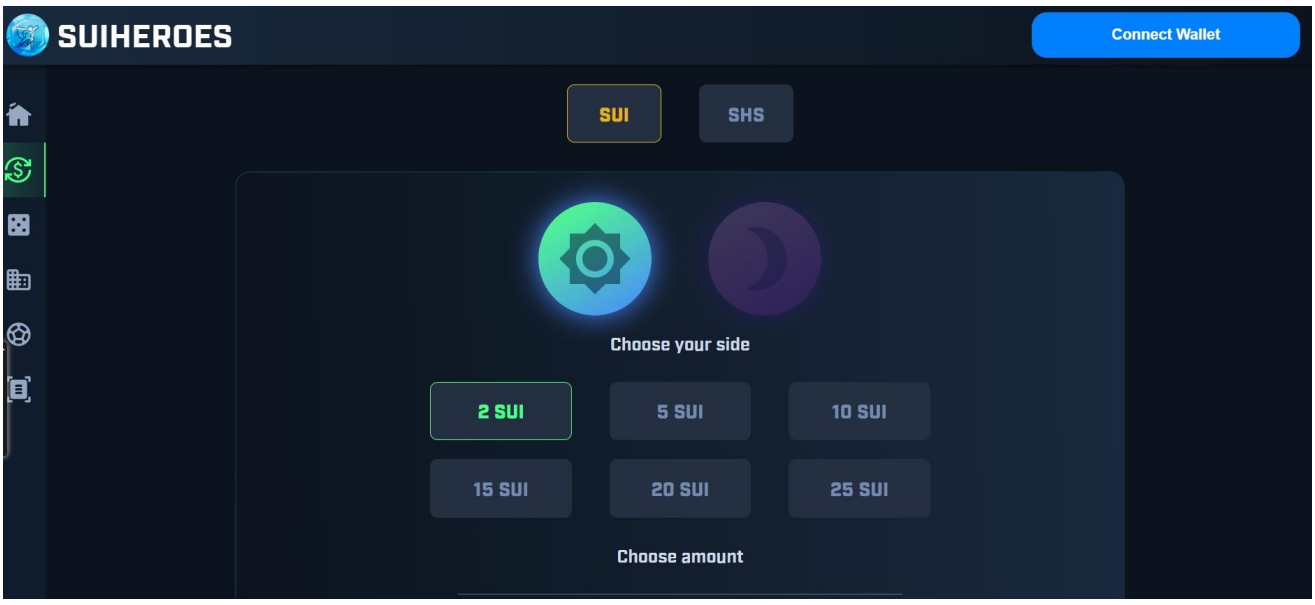
Coin Flip: This page describes how the Tower game works on the SUI Heroes platform.

Rules Of The Game

Coin Flip is a game played between two players.
You can choose to create a game with another, or you can choose to flip against our automated SUIHeroesbot.

To start, each player chooses a side of the coin, either 'Heads' or 'Tails', and places a wager.
Together the players' wagers form the 'Prize Pool' or 'Pot' for the game.
Once the players' guesses and wagers are locked in, a coin is flipped and the winner is determined.
The winner receives the winner's share of the prize pool and the loser does not receive anything.

The SUIHEROES Platform Is Launching On the SUI Network



ISSUES CHECKING STATUS

	Issue Description	Checking Status
1.	Compiler errors.	PASSED
2.	Race Conditions and reentrancy. Cross-Function Race Conditions.	PASSED
3.	Possible Delay In Data Delivery.	PASSED
4.	Oracle calls.	PASSED
5.	Front Running.	PASSED
6.	Move Dependency.	PASSED
7.	Integer Overflow And Underflow.	PASSED
8.	DoS with Revert.	PASSED
9.	Dos With Block Gas Limit.	PASSED
10.	Methods execution permissions.	PASSED
11.	Economy Model of the contract.	PASSED
12.	The Impact Of Exchange Rate On the sol Logic.	PASSED
13.	Private use data leaks.	PASSED
14.	Malicious Event log.	PASSED
15.	Scoping and Declarations.	PASSED
16.	Uninitialized storage pointers.	PASSED
17.	Arithmetic accuracy.	PASSED
18.	Design Logic.	PASSED
19.	Cross-Function race Conditions	PASSED
20.	Save Upon Move contract Implementation and Usage.	PASSED
21.	Fallback Function Security	PASSED

AUDIT RESULT

PASSED

SMART CONTRACT AUDIT OF SUIHEROES

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor

All of the initially minted assets are sent to the contract deployer when deploying the contract. This can be an issue as the deployer and/or contract owner can distribute tokens without consulting the community.

```
1: CopyLoc[5](Arg5: &mut TxContext)
    52: FreezeRef
    53: Call tx_context::sender(&TxContext): address
    54: StLoc[7](loc1: address)
    55: MoveLoc[4](Arg4: &Clock)
    56: Call clock::timestamp_ms(&Clock): u64
    57: LdU64(1)
```

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.

RECOMMENDATION

Deployer and/or contract owner private keys are secured carefully.

Please refer to PAGE-09 CENTRALIZED PRIVILEGES for a detailed understanding.

ALLEVIATION

The COINFLIP project team understands the centralization risk. Some functions are provided privileged access to ensure a good runtime behavior in the project

Identifier	Definition	Severity
COD-10	Third Party Dependencies	Minor

Smart contract is interacting with third party protocols e.g., Pancakeswap router, cashier contract, protections contract. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised, and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

RECOMMENDATION

Inspect and validate third party dependencies regularly, and mitigate severe impacts whenever necessary.

DISCLAIMERS

Vital Block provides the easy-to-understand audit of Solidity, Move and Raw 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 asset. 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, VITAL BLOCK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, VITAL BLOCK 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, VITAL BLOCK 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. Vital Block 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 Vital Block. 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 Vital block Security is not responsible for the content or operation of such websites and social accounts and that Vital Block 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 VITAL BLOCK

Vital Block provides intelligent blockchain Security Solutions. We provide solidity and Raw Code Review, testing, and auditing services. We have Partnered with 15+ Crypto Launchpads, audited 50+ smart contracts, and analyzed 200,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Aptos, Oasis, etc.

Vital Block is Dedicated to Making Defi & Web3 A Safer Place. We are Powered by Security engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 5 core members, and 4+ casual contributors.

Website: https://Vitalblock.org

Email: info@vitalblock.org

GitHub: https://github.com/vital-block

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

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

vital-block

info@vitalblock.org

www.Vitalblock.org

Vital Block Dedicated to securing Public and Private Blockchain Ecosystem