



Smart Contract Security Audit Report

Prepared for Sigma Money

Prepared by Supremacy

August 14, 2025

Contents

1	Introduction	3
1.1	About Client	4
1.2	Audit Scope	4
1.3	Changelogs	5
1.4	About Us	6
1.5	Terminology	6
2	Findings	7
2.1	Critical	8
2.2	High	9
2.3	Medium	13
2.4	Low	15
2.5	Informational	19
3	Disclaimer	23

1 Introduction

Given the opportunity to review the design document and related codebase of the Sigma Money, we outline in the report our systematic approach to evaluate potential security issues in the smart contract(s) implementation, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About Client

Sigma Money is bring binance launchpool yield to stablecoin hodlers via fx protocol.

Item	Description
Client	Sigma Money
Type	Smart Contract
Languages	Solidity
Platform	EVM-compatible

1.2 Audit Scope

In the following, we show the Git repository of reviewed file and the commit hash used in this security audit:

Version	Repository	Commit Hash
1	contracts	2ece4d41116e3dde886b19c9515fe9904080a697
2	contracts	8c0753a4c076183494daa0f89483be795133f450
3	contracts	a7047fba8f7c79f5b9dc8a83fc97c09da11a1bc4
4	contracts	9bdff0754d8257ce0a92cc542365a64aa759a024e
5	contracts	61beb0f47e7bef8b12ad5e4b180ab1917d9679f8
6	contracts	647307b9b2be25d678d7f3e69f91c80cad3fe200
7	contracts	98f829990cd869f8065f0ff8f6c1c77d0e4782d7
8	aladdin-v3-contracts	8b18687de48dc1c82e346a0858325c00ceffbc79
9	contracts	5f51e8c2a882724c86052857c6058f87edae8f35
10	contracts	dfcdcd9318080049f0e4553c1baf5b7ff76f4ee0
11	contracts	9fb1b2c95d4264365106467ac10da2214a15cb23
12	contracts	9b6406407cde12bf939e9f9f333effce8e69d147
13	contracts	c6c1169f45b8fb4d1e6be7d6aa709d713cad6c2c
14	contracts	ca6b68faa3eccf65cb49e8765f08568ae7ec2696
15	contracts	6ebf5e8d72fae96b35dfb20f8d3580bee3d90b1c
16	contracts	d2931e80a276825eeddaffd31fd8990692b03ef7

Notes: The 8th difference audit is based on the #bd19179 commit of the aladdin-v3-contracts repository. Meanwhile, the 9th to 16th difference audits are based on the #5f51e8c commit of the fx-protocol-contracts repository.

1.3 Changelogs

Version	Date	Description
0.1	May 07, 2025	Initial Draft
1.0	May 17, 2025	Final Release
1.1	June 17, 2025	Post-Final Release #1
1.2	July 01, 2025	Post-Final Release #2
1.3	July 03, 2025	Post-Final Release #3
1.4	July 22, 2025	Post-Final Release #4
1.5	August 11, 2025	Post-Final Release #5
1.6	August 14, 2025	Post-Final Release #6

1.4 About Us

Supremacy is a leading blockchain security firm, composed of industry hackers and academic researchers, provide top-notch security solutions through our technology precipitation and innovative research.

We are reachable at X (<https://x.com/SupremacyHQ>), or Email (contact@supremacy.email).

1.5 Terminology

For the purpose of this assessment, we adopt the following terminology. To classify the severity of our findings, we determine the likelihood and impact (according to the CVSS risk rating methodology).

- Likelihood represents the likelihood of a finding to be triggered or exploited in practice
- Impact specifies the technical and business-related consequences of a finding
- Severity is derived based on the likelihood and the impact

We categorize the findings into four distinct categories, depending on their severity. These severities are derived from the likelihood and the impact using the following table, following a standard risk assessment procedure.

		Severity		
		Critical	High	Medium
Impact	High	High	Medium	Low
	Medium	Medium	Low	Low
	Low	Low	Low	Low

Likelihood

High Medium Low

As seen in the table above, findings that have both a high likelihood and a high impact are classified as critical. Intuitively, such findings are likely to be triggered and cause significant disruption. Overall, the severity correlates with the associated risk. However, every finding's risk should always be closely checked, regardless of severity.

2 Findings

The table below summarizes the findings of the audit, including status and severity details.

ID	Severity	Description	Status
1	Critical	Potential theft of assets	Fixed
2	High	Potential denial of service due to lack of fees	Acknowledged
3	High	Potential denial of service due to logic issue	Fixed
4	High	Potential denial of service due to fees hardcoded	Fixed
5	High	Interest rate calculation error	Fixed
6	Medium	Lack of slippage check	Fixed
7	Medium	Potential arbitrage opportunity	Acknowledged
8	Low	Lack of necessary assertion	Acknowledged
9	Low	Use SafeERC20 library	Fixed
10	Low	Lack of address validation	Fixed
11	Low	Lack of nonReentrant modifier	Fixed
12	Low	Use Ownable2Step library	Fixed
13	Informational	Redundant code removal for self approval	Fixed
14	Informational	Immutable variables	Fixed
15	Informational	Follow the Check-Effects-Interactions Pattern	Fixed
16	Informational	Lack of ownership verification	Acknowledged
17	Informational	Lack of event record	Fixed
18	Informational	Lack of comment	Fixed
19	Informational	Lack of pause check for listaStakeManager	Fixed
20	Informational	Potential arbitrary external call	Acknowledged
21	Informational	Redundant state variable removal	Fixed
22	Informational	Merging redundant functions	Fixed
23	Informational	Adjusting the code order	Fixed

2.1 Critical

1. Potential theft of assets [Critical]

Severity: Critical

Likelihood: High

Impact: High

Status: Fixed

Description

The deposit function in the SigmaController contract enables users to deposit collateral (e.g., slisBNB) and mint debt assets (fxUSD) to facilitate the protocol's leverage and borrowing operations. However, a issue exists due to the lack of validation for fxUSD balance changes, allowing malicious actor to steal the entire fxUSD balance held by the contract. This flaw permits malicious actor to extract significantly more fxUSD than the legitimate newDebt amount, resulting in substantial financial losses.

```
41   function deposit(address _pool, uint256 amount, uint256 positionId, int256
42     newColl, int256 newDebt) external {
43     require(amount >= 0, "Amount must be greater than or equal to 0");
44     require(amount == uint256(newColl), "New collateral must be equal to
45       amount");
46     require(newDebt >= 0, "New debt must be greater than or equal to 0");
47
48     // transfer
49     IERC20(slisBNB).transferFrom(msg.sender, address(this), amount);
50     deposits[msg.sender] += amount;
51
52     // mint SigmaClisBNBSY
53     slisBNB.approve(address(sy), amount);
54     sy.deposit(address(this), address(slisBNB), amount, 0);
55
56     // deposit sy to fx pool
57     sy.approve(address(fxPoolManager), uint256(newColl));
58     uint256 positionId = fxPoolManager.operate(_pool, positionId, newColl,
59       newDebt);
60
61     // transfer fxUSD to the user
62     uint256 fxUSDOut = IERC20(IPool(_pool)).fxUSD().balanceOf(address(this));
63     IERC20(IPool(_pool).fxUSD()).approve(address(this), fxUSDOut);
64     IERC20(IPool(_pool).fxUSD()).transfer(msg.sender, fxUSDOut);
65 }
```

SigmaController.sol

Recommendation

Consider always verifying balance changes before and after.

2.2 High

2. Potential denial of service due to lack of fees [High]

Severity: High

Likelihood: High

Impact: Medium

Status: Acknowledged

Description

The deposit function in the SigmaController contract allows users to deposit collateral (e.g., slisBNB) and mint debt assets (fxUSD) to support the protocol's leverage and borrowing operations. However, a issue exists due to improper handling of protocol fees, which can lead to a denial of service. This flaw causes transactions to revert when users fail to provide sufficient slisBNB to cover both the collateral and protocol fees, preventing legitimate users from completing deposits and disrupting protocol functionality.

```
41   function deposit(address _pool, uint256 amount, uint256 positionId, int256
42     newColl, int256 newDebt) external {
43     require(amount >= 0, "Amount must be greater than or equal to 0");
44     require(amount == uint256(newColl), "New collateral must be equal to
45     amount");
46     require(newDebt >= 0, "New debt must be greater than or equal to 0");
47
48     // transfer
49     IERC20(slisBNB).transferFrom(msg.sender, address(this), amount);
50     deposits[msg.sender] += amount;
51
52     // mint SigmaClisBNBSY
53     slisBNB.approve(address(sy), amount);
54     sy.deposit(address(this), address(slisBNB), amount, 0);
55
56     // deposit sy to fx pool
57     sy.approve(address(fxPoolManager), uint256(newColl));
58     uint256 positionId = fxPoolManager.operate(_pool, positionId, newColl,
59     newDebt);
60
61     // transfer fxUSD to the user
62     uint256 fxUSDOut = IERC20(IPool(_pool)).fxUSD().balanceOf(address(this));
63     IERC20(IPool(_pool)).fxUSD().approve(address(this), fxUSDOut);
64     IERC20(IPool(_pool)).fxUSD().transfer(msg.sender, fxUSDOut);
65 }
```

SigmaController.sol

In the following, we show the operate function, responsible for processing the deposit and managing protocol fees, requires the caller SigmaController to transfer both the newColl and protocolFees.

Its relevant logic is implemented as follows:

```
128  ****
129  * Public Mutated Functions *
```

```

130     *****/
131
132     /// @inheritdoc IPoolManager
133     function operate(
134         address pool,
135         uint256 positionId,
136         int256 newColl,
137         int256 newDebt
138     ) external onlyRegisteredPool(pool) nonReentrant whenNotPaused returns
139     (uint256) {
140         address collateralToken = IPool(pool).collateralToken();
141         uint256 scalingFactor = _getTokenScalingFactor(collateralToken);
142
143         int256 newRawColl = newColl;
144         if (newRawColl != type(int256).min) {
145             newRawColl = _scaleUp(newRawColl, scalingFactor);
146         }
147
148         uint256 rawProtocolFees;
149         // the `newRawColl` is the result without `protocolFees`
150         (positionId, newRawColl, newDebt, rawProtocolFees) = IPool(pool).operate(
151             positionId,
152             newRawColl,
153             newDebt,
154             _msgSender()
155         );
156
157         newColl = _scaleDown(newRawColl, scalingFactor);
158         uint256 protocolFees = _scaleDown(rawProtocolFees, scalingFactor);
159         _changePoolDebts(pool, newDebt);
160         if (newRawColl > 0) {
161             _accumulatePoolOpenFee(pool, protocolFees);
162             _changePoolCollateral(pool, newColl, newRawColl);
163             IERC20(collateralToken).safeTransferFrom(_msgSender(), address(this),
164             uint256(newColl) + protocolFees);
165         } else if (newRawColl < 0) {
166             _accumulatePoolCloseFee(pool, protocolFees);
167             _changePoolCollateral(pool, newColl - int256(protocolFees), newRawColl -
168             int256(rawProtocolFees));
169             _transferOut(collateralToken, uint256(-newColl), _msgSender());
170         }
171
172         if (newDebt > 0) {
173             IFxUSDRegeneracy(fxUSD).mint(_msgSender(), uint256(newDebt));
174         } else if (newDebt < 0) {
175             IFxUSDRegeneracy(fxUSD).burn(_msgSender(), uint256(-newDebt));
176         }
177
178         emit Operate(pool, positionId, newColl, newDebt, protocolFees);
179
180         return positionId;
181     }

```

PoolManager.sol

Recommendation

Revise the code logic accordingly.

Feedback

When the user's balance is insufficient to deduct the processing fee, the transaction will be revert.

3. Potential denial of service due to logic issue [High]

Severity: High

Likelihood: High

Impact: Medium

Status: Fixed

Description

The deposit function in the SigmaController contract enables users to deposit collateral (e.g., slisBNB) and mint debt assets (fxUSD) to support the protocol's leverage and borrowing operations. A critical design flaw exists in the handling of NFT position transfers, specifically the `IERC721(_pool).transferFrom(address(this), msg.sender, positionId)` call, which reverts during the second deposit invocation for an existing position. This issue prevents users from updating or managing existing positions, leading to a denial of service condition that disrupts protocol functionality.

```
41   function deposit(address _pool, uint256 amount, uint256 positionId, int256
42     newColl, int256 newDebt) external {
43     require(amount >= 0, "Amount must be greater than or equal to 0");
44     require(amount == uint256(newColl), "New collateral must be equal to
45       amount");
46     require(newDebt >= 0, "New debt must be greater than or equal to 0");
47
48     // transfer
49     IERC20(slisBNB).transferFrom(msg.sender, address(this), amount);
50     deposits[msg.sender] += amount;
51
52     // mint SigmaClisBNBSY
53     slisBNB.approve(address(sy), amount);
54     sy.deposit(address(this), address(slisBNB), amount, 0);
55
56     // deposit sy to fx pool
57     sy.approve(address(fxPoolManager), uint256(newColl));
58     uint256 positionId = fxPoolManager.operate(_pool, positionId, newColl,
59     newDebt);
60
61     // transfer fxUSD to the user
62     uint256 fxUSDOut = IERC20(IPool(_pool).fxUSD()).balanceOf(address(this));
63     IERC20(IPool(_pool).fxUSD()).approve(address(this), fxUSDOut);
64     IERC20(IPool(_pool).fxUSD()).transfer(msg.sender, fxUSDOut);
65   }
```

SigmaController.sol

Recommendation

Revise the code logic accordingly.

4. Potential denial of service due to fees hardcoded [High]

Severity: High Likelihood: High Impact: Medium
Status: Fixed

Description

In the `SigmaController` contract, the `_convertSliSBNBToWBNB()` function facilitates token swaps from `sliSBNB` to `wBNB` via `pancakeSwapRouter::exactInputSingle()`. However, the pool fee is hardcoded to 100 (0.01%), without verifying whether the `sliSBNB/wBNB` pool uses this fee tier. PancakeSwap V3 supports multiple fee tiers (e.g., 100, 500, 3000, 10000, corresponding to 0.01%, 0.05%, 0.3%, 1%). If the pool's actual fee tier differs from the hardcoded value, the swap transaction will fail, causing a revert.

```
1033     function _convertSliSBNBToWBNB(uint256 sliSBNBAmount) internal returns
1034     (uint256 wBNBAmount) {
1035         sliSBNB.forceApprove(address(pancakeSwapRouter), sliSBNBAmount);
1036         IV3SwapRouter.ExactInputSingleParams memory params =
1037             IV3SwapRouter.ExactInputSingleParams(
1038                 address(sliSBNB),
1039                 address(wBNB),
1040                 100,
1041                 address(this),
1042                 sliSBNBAmount,
1043                 sliSBNBAmount, // amountOutMinimum
1044                 0
1045             );
1046         wBNBAmount = pancakeSwapRouter.exactInputSingle(params);
1047     }
```

SigmaController.sol

Recommendation

Revise the code logic accordingly.

Feedback

This function has been removed.

5. Interest Rate Calculation Error [High]

Severity: High Likelihood: High Impact: Medium
Status: Fixed

Description

The `PoolConfiguration` contract, migrated to the Venus protocol, contains a critical flaw in its interest rate calculation logic. The old contract calculated actual rate changes using Aave's `borrowIndex` with the formula `(newBorrowIndex - prevBorrowIndex) / prevBorrowIndex`, accurately reflecting dynamic market conditions. In contrast, the new contract relies solely on Venus's `borrowRatePerBlock`, computing annualized rates as `borrowRatePerBlock * BLOCKS_PER_MINUTE * MINUTES_PER_YEAR`, while hardcoding `BorrowRateSnapshot`'s `borrowIndex` to 0, ignoring Venus's available `borrowIndex`. This leads to inaccurate rate calculations that fail to capture real market dynamics. Additionally,

the hardcoded `BLOCKS_PER_MINUTE = 80` assumption may not align with BNB Chain's variable block times, causing rate miscalculations if actual block times deviate. Furthermore, the `_computeAverageInterestRate` function lacks smoothing for `borrowRatePerBlock`, making it vulnerable to manipulation from short-term market fluctuations. These issues can result in incorrect funding ratios in `getLongPoolFundingRatio` and `getShortPoolFundingRatio`, disrupting pool balance, potentially causing user fund losses, or abnormal trader profits.

Recommendation

Revise the code logic accordingly.

Feedback

The implementation described in the issue details has been updated. The current approach is the official implementation provided by the Venus technical team, where the block count per year is now also read from the contract.

2.3 Medium

6. Lack of slippage check [Medium]

Severity: Medium

Likelihood: Medium

Impact: Medium

Status: Fixed

Description

The `SigmaController` contract facilitates token swaps through the `_swap()` function, which interacts with external swap targets (e.g., decentralized exchanges) to convert input tokens to output tokens, such as during collateral conversion in the `_transferInCollAndConvert()` function. However, the `_swap()` function does not implement slippage protection, which is a critical safeguard in decentralized finance (DeFi) protocols. Slippage protection ensures that the amount of output tokens received from a swap meets a minimum threshold, preventing users from receiving significantly fewer tokens than expected due to price volatility or front-running attacks like Miner Extractable Value (MEV). The contract defines constants `MAX_SLIPPAGE` (10%) and `MIN_SLIPPAGE` (0.01%), indicating an intention to handle slippage tolerance, but these are not utilized in the `_swap()` function. Without enforcing a minimum output amount, users are exposed to potential losses if the market price moves unfavorably during the transaction, especially in volatile markets or low-liquidity pools. This issue affects the `deposit()` function, where collateral tokens are swapped to `slisBNB`, and potentially other operations relying on `_swap()`. The lack of slippage checks could lead to financial losses for users and undermine trust in the protocol.

```
41  /// @dev Internal function to do swap.
42  /// @param tokenIn The address of input token.
43  /// @param tokenOut The address of output token.
44  /// @param amountIn The amount of input token.
45  /// @param swapTarget The address of target contract used for swap.
46  /// @param swapData The calldata passed to target contract.
47  /// @return amountOut The amount of output tokens received.
```

```

48 function _swap(
49     address tokenIn,
50     address tokenOut,
51     uint256 amountIn,
52     address swapTarget,
53     bytes memory swapData
54 ) internal returns (uint256 amountOut) {
55     _onlySupportedSwapTarget(swapTarget);
56
57     if (amountIn == 0) return 0;
58
59     amountOut = _balanceOf(tokenOut, address(this));
60     if (tokenIn != address(0)) {
61         IERC20(tokenIn).forceApprove(swapTarget, amountIn);
62         (bool success, ) = swapTarget.call(swapData);
63         // below lines will propagate inner error up
64         if (!success) {
65             // solhint-disable-next-line no-inline-assembly
66             assembly {
67                 let ptr := mload(0x40)
68                 let size := returndatasize()
69                 returndatacopy(ptr, 0, size)
70                 revert(ptr, size)
71             }
72         }
73     } else {
74         (bool success, ) = swapTarget.call{ value: amountIn }(swapData);
75         if (!success) {
76             // solhint-disable-next-line no-inline-assembly
77             assembly {
78                 let ptr := mload(0x40)
79                 let size := returndatasize()
80                 returndatacopy(ptr, 0, size)
81                 revert(ptr, size)
82             }
83         }
84     }
85     amountOut = _balanceOf(tokenOut, address(this)) - amountOut;
86 }
```

SigmaController.sol

Recommendation

Revise the code logic accordingly.

7. Potential arbitrage opportunity [Medium]

Severity: Medium

Likelihood: Medium

Impact: Medium

Status: Acknowledged

Description

The SigmaSPAdapter contract's `convertToDeposit()` and `convertToRedeem()` functions handle transactions in opposite directions. The `convertToDeposit()` swaps `tokenIn` for `SP` on a 1:1 basis, while `convertToRedeem()` converts `tokenOut` back to `tokenIn` through a liquidity pool. However, the liquidity pool does not follow a 1:1 exchange rule, which creates potential arbitrage opportunities.

```
24     function convertToDeposit(
25         address tokenIn,
26         uint256 amountTokenIn
27     ) external override returns (uint256 amountOut) {
28         _validAdapterTokenIn(tokenIn);
29
30         IERC20(tokenIn).forceApprove(SP, amountTokenIn);
31         amountOut = ISigmaSP(SP).deposit(msg.sender, tokenIn, amountTokenIn,
32         0);
33     }
34
35     function convertToRedeem(
36         address tokenOut,
37         uint256 amountPivotToken
38     ) external override returns (uint256 amountOut) {
39         _validAdapterTokenOut(tokenOut);
40
41         uint256 minOut = (amountPivotToken *
42             (SLIPPAGE_PRECISION - CURVE_POOL_EXCHANGE_SLIPPAGE)) /
43             SLIPPAGE_PRECISION;
44         IERC20(SP).forceApprove(CURVE_POOL, amountPivotToken);
45         amountOut = ICurveStableSwapNG(CURVE_POOL).exchange(
46             1,
47             0,
48             amountPivotToken,
49             minOut,
50             msg.sender
51         );
52     }
53 }
```

SigmaSPAdapter.sol

Recommendation

Revise the code logic accordingly.

2.4 Low

8. Lack of necessary assertion [Low]

Severity: Low

Likelihood: Low

Impact: Low

Status: Acknowledged

Description

In the `SigmaController::deposit()` function, it enables users to deposit collateral (e.g., `slisBNB`) and mint debt assets (`fxUSD`) to support the protocol's leverage and borrowing operations. Due to the absence of validation to ensure that the `fxUSD` amount transferred to the user (`fxUSDOut`) equals the minted debt amount (`newDebt`). The function transfers the entire `fxUSD` balance of the contract without checking if it matches `newDebt`, which could lead to unintended transfers of excess `fxUSD` if the contract holds additional `fxUSD` from other operations. This could result in minor financial discrepancies or user confusion, though the impact is limited under normal protocol conditions.

```

41   function deposit(address _pool, uint256 amount, uint256 positionId, int256
42     newColl, int256 newDebt) external {
43     require(amount >= 0, "Amount must be greater than or equal to 0");
44     require(amount == uint256(newColl), "New collateral must be equal to
45       amount");
46     require(newDebt >= 0, "New debt must be greater than or equal to 0");
47
48     // transfer
49     IERC20(slisBNB).transferFrom(msg.sender, address(this), amount);
50     deposits[msg.sender] += amount;
51
52     // mint SigmaClisBNBSY
53     slisBNB.approve(address(sy), amount);
54     sy.deposit(address(this), address(slisBNB), amount, 0);
55
56     // deposit sy to fx pool
57     sy.approve(address(fxPoolManager), uint256(newColl));
58     uint256 positionId = fxPoolManager.operate(_pool, positionId, newColl,
59     newDebt);
60
61     // transfer fxUSD to the user
62     uint256 fxUSDOut = IERC20(IPool(_pool)).balanceOf(address(this));
63     IERC20(IPool(_pool)).fxUSD().approve(address(this), fxUSDOut);
64     IERC20(IPool(_pool)).fxUSD().transfer(msg.sender, fxUSDOut);
65 }
```

SigmaController.sol

Recommendation

Revise the code logic accordingly.

9. Use SafeERC20 library [Low]

Severity: Low

Likelihood: Low

Impact: Low

Status: Fixed

Description

To ensure robust and secure interaction with ERC20 tokens, it is recommended to use OpenZeppelin's `SafeERC20` library. The library provides wrapper functions that contain additional checks and protections to ensure that token transfers and other operations are performed safely and correctly.

Recommendation

It is recommended to use the SafeERC20 method transfer and transferFrom, instead of unsafe transfer and transferFrom.

10. Lack of address validation [Low]

Severity: Low

Likelihood: Low

Impact: Low

Status: Fixed

Description

In the SigmaController contract, several functions lack zero-address validation.

```
41     function deposit(address _pool, uint256 amount, uint256 positionId, int256
42         newColl, int256 newDebt) external {
43         require(amount >= 0, "Amount must be greater than or equal to 0");
44         require(amount == uint256(newColl), "New collateral must be equal to
45             amount");
46         require(newDebt >= 0, "New debt must be greater than or equal to 0");
47
48         // transfer
49         IERC20(slisBNB).transferFrom(msg.sender, address(this), amount);
50         deposits[msg.sender] += amount;
51
52         // mint SigmaClisBNBSY
53         slisBNB.approve(address(sy), amount);
54         sy.deposit(address(this), address(slisBNB), amount, 0);
55
56         // deposit sy to fx pool
57         sy.approve(address(fxPoolManager), uint256(newColl));
58         uint256 positionId = fxPoolManager.operate(_pool, positionId, newColl,
59             newDebt);
60
61         // transfer fxUSD to the user
62         uint256 fxUSDOut = IERC20(IPool(_pool)).fxUSD().balanceOf(address(this));
63         IERC20(IPool(_pool)).fxUSD().approve(address(this), fxUSDOut);
64         IERC20(IPool(_pool)).fxUSD().transfer(msg.sender, fxUSDOut);
65
66         // transfer xBNB to the user
67         IERC721(_pool).transferFrom(address(this), msg.sender, positionId);
68     }
69
70     function redeem(address _pool, uint256 amount, uint256 positionId, int256
71         newColl, int256 newDebt) external {
72         // check if the user has enough deposits
73         require(deposits[msg.sender] >= amount, "Insufficient deposits");
74         require(amount >= 0, "Amount must be greater than or equal to 0");
75         require(amount == uint256(-newColl), "New collateral absolute value must be
76             equal to amount");
77         require(newDebt <= 0, "New debt must be less than or equal to 0");
78
79         if (newDebt < 0) {
80             // transfer fxUSD to this contract
81             IERC20(IPool(_pool)).fxUSD().transferFrom(msg.sender, address(this),
82                 uint256(-newDebt));
83             IERC20(IPool(_pool)).fxUSD().approve(address(fxPoolManager), uint256(-
84                 newDebt));
85     }
```

```

78     }
79
80     // transfer xBNB to this contract
81     IERC721(_pool).transferFrom(msg.sender, address(this), positionId);
82
83     // withdraw sy from fx pool
84     uint256 syBalance = sy.balanceOf(address(this));
85     fxPoolManager.operate(_pool, positionId, newColl, newDebt);
86     uint256 syDelta = sy.balanceOf(address(this)) - syBalance;
87
88     // transfer fxUSD to the user
89     IERC721(_pool).transferFrom(address(this), msg.sender, positionId);
90
91     if (syDelta > 0) {
92         // burn sy, redeem slisBNB
93         sy.redeem(address(this), syDelta, address(slisBNB), 0, false);
94
95         // transfer slisBNB to user and update deposits
96         slisBNB.transfer(msg.sender, syDelta);
97     }
98
99     deposits[msg.sender] -= amount;
100 }
```

SigmaController.sol

Recommendation

Consider adding zero address validation

11. Lack of nonReentrant modifier [Low]

Severity: Low

Likelihood: Low

Impact: Low

Status: Fixed

Description

In the SigmaController contract, several functions involves an external call. There are no obvious issues in the current implementation, but to increase security and prevent unexpected behavior, it is a good idea to include the `nonReentrant` modifier. This is a safer approach and prevents potential issues in the event of future updates or unexpected situations.

Recommendation

Add a `nonReentrant` type modifier to the functions to further improve security.

12. Use Ownable2Step library [Low]

Severity: Low

Likelihood: Low

Impact: Low

Status: Fixed

Description

A single-step ownership transfer means that if an incorrect address is passed when transferring ownership or administrative privileges, it means that the role will be lost forever. The ownership model for this protocol is implemented in `Ownable.sol`, which implements single-step transfers. This can cause problems for all methods marked as `onlyOwner` throughout the protocol, some of which are core functionality of the protocol.

Recommendation

A two-step ownership transfer model is recommended, where the ownership transfer is pending and the new owner should assert its new rights, otherwise the old owner remains in control of the contract. Consider using OpenZeppelin's `Ownable2Step` contract.

2.5 Informational

13. Redundant code removal for self approval [Informational]

Status: Fixed

Description

In the `SigmaController::deposit` function, it approves the `SigmaController` contract itself (`address(this)`) to manage `fxUSDOut` amount of `fxUSD` tokens. However, the subsequent transfer operation, `IERC20(IPool(_pool).fxUSD()).transfer(msg.sender, fxUSDOut)`, does not require any approve. Thus, this approve call is redundant.

```
60     IERC20(IPool(_pool).fxUSD()).approve(address(this), fxUSDOut);
```

`SigmaController.sol`

Recommendation

Revise the code logic accordingly.

14. Immutable variables [Informational]

Status: Fixed

Description

Variables such as `sIsBNB`, `sy`, `sIsBNBProvider`, `fxPoolManager` and `listalpDelegateTo` are defined only in the `constructor()`. Therefore, it can be `immutable`, since immutable values are cheaper to read.

Recommendation

Consider making variables immutable.

15. Follow the Check-Effects-Interactions Pattern [Informational]

Status: Fixed

Description

In the `deposit` and `redeem` functions of the `SigmaController` contract, the control flow does not follow the check-effects-interact pattern.

Recommendation

Revise the code logic accordingly.

16. Lack of ownership verification [Informational]

Status: Acknowledged

Description

Lack of ownership verification of positionId in the deposit and redeem functions of SigmaController contract.

Recommendation

Revise the code logic accordingly.

17. Lack of event record [Informational]

Status: Fixed

Description

In the SigmaController contract, the deposit() and redeem() functions are missing event records. However, events are important because off-chain monitoring tools rely on them to index important state changes to the smart contract(s).

Recommendation

Always ensure that all functions that trigger state changes have event logging capabilities.

18. Lack of comment [Informational]

Status: Fixed

Description

Throughout the codebase there are numerous functions missing or lacking documentation. This hinders reviewers' understanding of the code's intention, which is fundamental to correctly assess not only security, but also correctness. Additionally, comments improve readability and ease maintenance. They should explicitly explain the purpose or intention of the functions, the scenarios under which they can fail, the roles allowed to call them, the values returned and the events emitted.

Recommendation

Consider thoroughly documenting all functions (and their parameters) that are part of the smart contracts' public interfaces. Functions implementing sensitive functionality, even if not public, should be clearly documented as well. When writing comments, consider following the Ethereum Natural Specification Format (NatSpec).

19. Lack of pause check for listaStakeManager [Informational]

Status: Fixed

Description

In the `SigmaController` contract, there is a lack of pause checks for the `requestWithdraw()` and `claimWithdraw()` functions of `listaStakeManager`. If the contract is in a paused state, this could lead to unnecessary gas consumption.

Recommendation

Revise the code logic accordingly.

20. Potential arbitrary external call [Informational]

Status: Acknowledged

Description

The `_swap` function in the `SigmaController` contract allows the execution of arbitrary external calls to a `swapTarget` address via low-level call (i.e., `swapTarget.call(swapData)`). While the function restricts `swapTarget` to addresses listed in the `supportedSwapTargets` whitelist, this mechanism is insufficient to mitigate the risks associated with arbitrary external calls. The following issues could lead to arbitrary theft of unlimited approval user assets.

Recommendation

Strictly scrutinize the whitelists.

21. Redundant state variable removal [Informational]

Status: Fixed

Description

The constants `MAX_SLIPPAGE` and `MIN_SLIPPAGE` defined by the `SigmaController` contract are not used efficiently.

Recommendation

Consider removing redundant code.

22. Merging redundant functions [Informational]

Status: Fixed

Description

The `registerSwapTarget()` and `unregisterSwapTarget()` functions can be combined into a single function.

```
233     function registerSwapTarget(address swapTarget) external onlyOwner {
234         supportedSwapTargets[swapTarget] = true;
235     }
236
237     function unregisterSwapTarget(address swapTarget) external onlyOwner {
238         require(supportedSwapTargets[swapTarget], "Swap target not registered");
239         delete supportedSwapTargets[swapTarget];
240     }
```

SigmaController.sol

Recommendation

Revise the code logic accordingly.

23. Adjusting the code order [Informational]

Status: Fixed

Description

The `ListaStrategy::deposit()` function counts before depositing, and does not follow the Checks-Effects-Interactions pattern.

```
34     function deposit(uint256 amount) external onlyOperator {  
35         unchecked {  
36             principal += amount;  
37         }  
38         IMoolahVault(POOL).deposit(amount, address(this));  
39     }
```

ListaStrategy.sol

Recommendation

Revise the code logic accordingly.

3 Disclaimer

This security audit report does not constitute investment advice or a personal recommendation. It does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. Any entity should not rely on this report in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. This security audit report is not an endorsement of any particular project or team, and the report does not guarantee the security of any particular project. This audit does not give any warranties on discovering all security issues of the smart contracts, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues, also cannot make guarantees about any additional code added to the assessed project after the audit version. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with independent audits and a public bug bounty program to ensure the security of smart contract(s). Unless explicitly specified, the security of the language itself (e.g., the solidity language), the underlying compiling toolchain and the computing infrastructure are out of the scope.

