SMART CONTRACT AUDIT REPORT

for

RockX DirectStaking

Prepared By: Xiaomi Huang

PeckShield
March 14, 2023

Document Properties

Client	RockX
Title	Smart Contract Audit Report
Target	RockX DirectStaking
Version	1.0
Author	Xuxian Jiang
Auditors	Luck Hu, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	March 14, 2023	Xuxian Jiang	Final Release
1.0-rc	March 10, 2023	Luck Hu	Release Candidate #1

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related source code of the `DirectStaking` support in `RockX`, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, 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 RockX

`RockX` is a blockchain fintech company that helps users embrace `Web 3.0` effortlessly through the development of innovative products and infrastructure. It also strives to enable institutions and disruptors in the financial and Internet sectors to gain seamless access to blockchain data, crypto yield products and best-in-class key management solutions in a sustainable way. The audited `DirectStaking` support makes it possible for anyone to combine multiple deposits to the `Beacon` chain deposit contract in one single transaction, and join the fee rewards pool where user can claim its rewards share. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of The RockX DirectStaking

Item	Description
Name	RockX
Website	https://www.rockx.com/
Type	EVM Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	March 14, 2023

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit.

- https://github.com/RockX-SG/direct_staking_contracts.git (82a5f16)

And here is the commit ID after fixes for the issues found in the audit have been checked in:

- https://github.com/RockX-SG/direct_staking_contracts.git (218945f)

1.2 About PeckShield

PeckShield Inc. [7] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Likelihood

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [6]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.

- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.

- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [5], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 | Findings

2.1 Summary

Here is a summary of our findings after analyzing the implementation of the `DirectStaking` of `RockX`. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	1	■
Low	1	■
Informational	0	
Total	2	

We have so far identified a list of potential issues. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities that need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 1 medium-severity vulnerability and 1 low-severity vulnerability.

Table 2.1: Key RockX DirectStaking Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Potential Signatures Malleability in verifySigner()	Business Logic	Fixed
PVE-002	Medium	Trust Issue of Admin Keys	Security Features	Mitigated

Besides recommending specific countermeasures to mitigate these issues, we also emphasize that it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms need to kick in at the very moment when the contracts are being deployed in mainnet. Please refer to Section 3 for details.

3 Detailed Results

3.1 Potential Signatures Malleability in verifySigner()

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: High
- Target: DirectStaking
- Category: Business Logic [4]
- CWE subcategory: CWE-841 [2]

Description

The audited DirectStaking contract has a _digest() routine that is used to generate the hashed message per the input parameters. The hashed message is used to recover and verify the signer with the signature in the verifySigner() routine.

Within the _digest() routine, the current implementation makes use of address(this) (line 417) as the domain separator which could prevent a valid signature signed for one contract to be replayed on the other. However, we notice the current implementation can be improved by adding block.chainid as part of the domain separator. Suppose there is a hard-fork, a valid signature for one chain could be replayed on the other.

```
410     function _digest(
411         uint256 extraData,
412         address claimaddr,
413         address withdrawaddr,
414         bytes[] calldata pubkeys,
415         bytes[] calldata signatures) private view returns (bytes32) {
416 
417         bytes32 digest = sha256(abi.encode(extraData, address(this), claimaddr,
            withdrawaddr));
418 
419         for (uint i=0;i<pubkeys.length;i++) {
420             digest = sha256(abi.encode(digest, pubkeys[i], signatures[i]));
421         }
422 
423         return digest;
```

```
    }
```

Listing 3.1: `DirectStaking::_digest()`

What's more, the `verifySigner()` routine accepts the input signature in the format of `bytes` (line 193), and it uses the `ECDSA` library of `OpenZeppelin` to recover the signer (line 197). However, we notice in `release-4.7.3` of `OpenZeppelin`, there's a breaking change which no longer accepts compact signatures in `recover(bytes32,bytes)` to prevent malleability. Based on this, it's suggested to use a newer `OpenZeppelin` release since `release-4.7.3`, or use the `(v,r,s)` format of signatures.

```
187     function verifySigner(
188         uint256 extraData,
189         address claimaddr,
190         address withdrawaddr,
191         bytes[] calldata pubkeys,
192         bytes[] calldata signatures,
193         bytes calldata paramsSig) public view returns(bool) {
194 
195         // params signature verification
196         bytes32 digest = ECDSA.toEthSignedMessageHash(_digest(extraData, claimaddr,
                withdrawaddr, pubkeys, signatures));
197         address signer = ECDSA.recover(digest, paramsSig);
198 
199         return (signer == sysSigner);
200     }
```

Listing 3.2: `DirectStaking::verifySigner()`

Recommendation Add `block.chainid` as part of the domain separator and use a newer `OpenZeppelin` release since `release-4.7.3`.

Status The issue has been fixed by this commit: `218945f`, and the team confirms they are using `release-4.8.0`.

3.2 Trust Issue of Admin Keys

- ID: PVE-002
- Severity: Medium
- Likelihood: Low
- Impact: High
- Target: `Multiple contracts`
- Category: Security Features [3]
- CWE subcategory: CWE-287 [1]

Description

In `DirectStaking`, there is a privileged administrative account (the account with the `DEFAULT_ADMIN_ROLE` role). The administrative account plays a critical role in governing and regulating the staking-wide operations. Our analysis shows that this privileged account needs to be scrutinized. In the following, we use the `DirectStaking` contract as an example and show the representative functions potentially affected by the privileges of the administrative account.

Specifically, the privileged functions in `DirectStaking` allow for the `DEFAULT_ADMIN_ROLE` role to set the `sysSigner` which can sign staking messages, set the `ethDepositContract` which accepts user deposits, etc.

```
     /**
      * @dev set signer address
      */
    function setSigner(address _signer) external onlyRole(DEFAULT_ADMIN_ROLE) {
        sysSigner = _signer;

        emit SignerSet(_signer);
    }

    /**
     * @dev set reward pool contract address
     */
    function setRewardPool(address _rewardPool) external onlyRole(DEFAULT_ADMIN_ROLE) {
        rewardPool = _rewardPool;

        emit RewardPoolContractSet(_rewardPool);
    }

    /**
     * @dev set eth deposit contract address
     */
    function setETHDepositContract(address _ethDepositContract) external onlyRole(
        DEFAULT_ADMIN_ROLE) {
        ethDepositContract = _ethDepositContract;

        emit DepositContractSet(_ethDepositContract);
    }
```

Listing 3.3: Example Privileged Operations in `DirectStaking`

We understand the need of the privileged functions for contract maintenance, but at the same time the extra power to the administrative account may also be a counter-party risk to the protocol users. It would be worrisome if the privileged administrative account is a plain EOA account. Note that a multi-sig account could greatly alleviate this concern, though it is still far from perfect. Specifically, a better approach is to eliminate the administration key concern by transferring the role to a community-governed DAO.

Recommendation Promptly transfer the privileged account to the intended `DAO`-like governance contract. All changes to privileged operations may need to be mediated with necessary timelocks. Eventually, activate the normal on-chain community-based governance life-cycle and ensure the intended trustless nature and high-quality distributed governance.

Status This issue has been mitigated as the team confirms that all the privileged roles will be transferred to `Gnosis multi-sig`.

4 Conclusion

In this audit, we have analyzed the design and implementation of the `DirectStaking` support in `RockX`, which makes it possible for anyone to combine multiple deposits to the `Beacon` chain deposit contract in one single transaction, and join the fee rewards pool where user can claim its rewards share. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that `Solidity`-based smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[2] MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

[3] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[4] MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

[5] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[6] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[7] PeckShield. PeckShield Inc. https://www.peckshield.com.