SMART CONTRACT AUDIT REPORT

for

UXLINK Reward Pool

Prepared By: Xiaomi Huang

PeckShield
November 8, 2024

Document Properties

Client	UXLINK
Title	Smart Contract Audit Report
Target	UXLINK Reward Pool
Version	1.0
Author	Xuxian Jiang
Auditors	Daisy Cao, Xuxian Jiang
Reviewed by	Xuxian Jiang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	November 8, 2024	Xuxian Jiang	Final Release
1.0-rc	November 8, 2024	Xuxian Jiang	Release Candidate

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 `UXLINK Reward Pool` smart contract, 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 UXLINK Reward Pool

`UXLINK` aims to be the largest `Web3` social platform and infrastructure for users and developers to discover, distribute, and trade crypto assets in unique social and group-based manner. This specific audit focuses on its staking contract to reward staking users. The basic information of the audited contract is as follows:

Table 1.1: Basic Information of The `UXLINK Reward Pool` Contract

Item	Description
Name	UXLINK Reward Pool
Type	Ethereum Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	November 8, 2024

In the following, we show the deployment address of the audited contract.

- https://sepolia.arbiscan.io/address/0x14462F5501fFF2842Af14c2721596De3Ba4f502e

And here are the new deployment addresses of the audited contract after all fixes have been checked in:

- https://sepolia.arbiscan.io/address/0x5720266683F564cfe682a3Cb88ac289c327EFc4b
- https://arbiscan.io/address/0x5720266683F564cfe682a3Cb88ac289c327EFc4b
- https://arbiscan.io/address/0x3BA6a815E11a7842ADfca0E96e22343172db761B

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

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 `UXLINK Reward Pool` implementation. 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	2	■■
Low	0	
Informational	1	■
Total	3	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. 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 2 medium-severity vulnerabilities and 1 informational recommendation.

Table 2.1: Key UXLINK Reward Pool Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Possible Blocked Withdrawal Under Insufficient Surplus	Coding Practice	Resolved
PVE-002	Informational	Accommodation of Non-ERC20-Compliant Tokens	Business Logic	Resolved
PVE-003	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 Possible Blocked Withdrawal Under Insufficient Surplus

- ID: PVE-001
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: UXLINKTokenRewardPoolMultiple
- Category: Business Logic [4]
- CWE subcategory: CWE-841 [2]

Description

The `UXLINKTokenRewardPoolMultiple` contract supports standard staking features and allows users to stake and unstake their funds. While reviewing current unstaking logic, we notice an issue that may result in unstaking failure.

To elaborate, we show below the implementation of the related `withdraw()` routine as well as the associated `checkNextEpoch` modifier. We notice the associated modifier has a requirement, i.e., `require(poolSurplusReward >= nextCycleReward)` (line 177), which may revert the withdraw operation if current surplus reward is not able to support the next cycle reward. This revert unfortunately blocks users funds from being withdrawn.

```
    function withdraw(
        uint256 amount,
        uint256 positionID
    ) external updateReward(msg.sender) checkNextEpoch nonReentrant {
        require(
            withdrawOpened,
            "Have not opened"
        );
        require(
            amount > MIN_WITHDRAW_AMOUNT,
            "Withdraw amount must be greater than MIN_WITHDRAW_AMOUNT"
        );
        ...
    }
```

Listing 3.1: `UXLINKTokenRewardPoolMultiple::withdraw()`

```
    modifier checkNextEpoch() {
        if (block.timestamp >= periodFinish) {
            curCycleReward = nextCycleReward;
            require(
                poolSurplusReward >= nextCycleReward,
                "poolSurplusReward is not enough"
            );
            poolSurplusReward = poolSurplusReward - nextCycleReward;
            curCycleStartTime = block.timestamp;
            periodFinish = block.timestamp + (nextDuration);
            cycleTimes++;
            lastUpdateTime = curCycleStartTime;
            rewardRate = curCycleReward / (nextDuration);
            totalReward = totalReward + (curCycleReward);
            emit StartNewEpoch(curCycleReward, nextDuration);
        }
        _;
    }
```

Listing 3.2: `UXLINKTokenRewardPoolMultiple::checkNextEpoch()`

Recommendation Properly revise the above routines to ensure the user staked funds can be reliably withdrawn in all cases.

Status The issue has been resolved by following the above suggestion.

3.2 Accommodation of Non-ERC20-Compliant Tokens

- ID: PVE-002
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: `Multiple Contracts`
- Category: Business Logic [4]
- CWE subcategory: CWE-841 [2]

Description

Though there is a standardized ERC-20 specification, many token contracts may not strictly follow the specification or have additional functionalities beyond the specification. In the following, we examine the `transfer()` routine and related idiosyncrasies from current widely-used token contracts.

In particular, we use the popular token, i.e., `ZRX`, as our example. We show the related code snippet below. On its entry of `transfer()`, there is a check, i.e., `if (balances[msg.sender] >= _value && balances[_to] + _value >= balances[_to])`. If the check fails, it returns `false`. However, the transaction still proceeds successfully without being reverted. This is not compliant with the ERC20 standard and may cause issues if not handled properly. Specifically, the ERC20 standard specifies the following: *"Transfers _value amount of tokens to address _to, and MUST fire the Transfer event. The function SHOULD throw if the message caller's account balance does not have enough tokens to spend."*

```
    function transfer(address _to, uint _value) returns (bool) {
        //Default assumes totalSupply can't be over max (2^256 - 1).
        if (balances[msg.sender] >= _value && balances[_to] + _value >= balances[_to]) {
            balances[msg.sender] -= _value;
            balances[_to] += _value;
            Transfer(msg.sender, _to, _value);
            return true;
        } else { return false; }
    }

    function transferFrom(address _from, address _to, uint _value) returns (bool) {
        if (balances[_from] >= _value && allowed[_from][msg.sender] >= _value &&
            balances[_to] + _value >= balances[_to]) {
            balances[_to] += _value;
            balances[_from] -= _value;
            allowed[_from][msg.sender] -= _value;
            Transfer(_from, _to, _value);
            return true;
        } else { return false; }
    }
```

Listing 3.3: ZRX::**transfer**()/transferFrom()

Because of that, a normal call to `transfer()` is suggested to use the safe version, i.e., `safeTransfer()`, In essence, it is a wrapper around ERC20 operations that may either throw on failure or return false without reverts. Moreover, the safe version also supports tokens that return no value (and instead revert or throw on failure). Note that non-reverting calls are assumed to be successful. Similarly, there is a safe version of `approve()/transferFrom()` as well, i.e., `safeApprove()/safeTransferFrom()`.

In the following, we show the `safeTokenTransfer()` routine in the `UXLINKTokenRewardPoolMultiple` contract. If the `USDT` token is supported as `rewardToken`, the unsafe version of `IERC20(rewardToken).transfer(_to, tokenBalance)` (line 442) may revert as there is no return value in the `USDT` token contract's `transferFrom()` implementation (but the `IERC20` interface expects a return value)!

```
438     function safeTokenTransfer(address _to, uint256 _amount) internal {
439         require(rewardToken != address(0x0), "No harvest began");
440         uint256 tokenBalance = IERC20(rewardToken).balanceOf(address(this));
441         if (_amount > tokenBalance) {
442             IERC20(rewardToken).transfer(_to, tokenBalance);
443         } else {
444             IERC20(rewardToken).transfer(_to, _amount);
445         }
446     }
```

Listing 3.4: `UXLINKTokenRewardPoolMultiple::safeTokenTransfer()`

Recommendation Accommodate the above-mentioned idiosyncrasy about ERC20-related `approve()/transfer()/transferFrom()`.

Status This issue has been resolved by following the above suggestion.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `UXLINKTokenRewardPoolMultiple`
- Category: Security Features [3]
- CWE subcategory: CWE-287 [1]

Description

In the `UXLINKTokenRewardPoolMultiple` contract, there is a privileged account, i.e., `manager`, which plays a critical role in governing and regulating the staking-wide operations (e.g., parameter setting and reward token adjustment). It also has the privilege to affect the flow of assets managed by this protocol. Our analysis shows that the privileged account needs to be scrutinized. In the following, we examine the privileged account and their related privileged accesses in current contracts.

```
    function notifyMintAmount(uint256 addNextReward) external onlyManager {
        uint256 balanceBefore = IERC20(rewardToken).balanceOf(address(this));
        IERC20(rewardToken).safeTransferFrom(
            msg.sender,
            address(this),
            addNextReward
        );
        uint256 balanceEnd = IERC20(rewardToken).balanceOf(address(this));

        poolSurplusReward = poolSurplusReward + (balanceEnd - balanceBefore);
        emit AddNextCycleReward(poolSurplusReward);
    }

    function setNextCycleReward(
        uint256 _nextCycleReward,
        uint256 _nextDuration
    ) external onlyManager {
        nextCycleReward = _nextCycleReward;
        nextDuration = _nextDuration;
        emit SetRewardConfig(nextCycleReward, nextDuration);
    }

    function setStakeTimeRatio(
        uint256[] memory _stakeTimeRatio
    ) external onlyManager {
        require( _stakeTimeRatio.length<=36, "stakeTimeRatio length is invalid!");
```

```
        stakeTimeRatio = _stakeTimeRatio;
        emit SetStakeTimeRatio(_stakeTimeRatio);
    }

    function setPunishRate(uint256 _punishRate) external onlyManager {
        punishRate = _punishRate;
        emit SetPunishRate(_punishRate);
    }

    function setWithdrawOpened(bool _opened) external onlyManager {
        withdrawOpened = _opened;
    }
```

Listing 3.5: Example Privileged Operations in the UXLINKTokenRewardPoolMultiple Contract

If the privileged admins are managed by a plain EOA account, this may be worrisome and pose counter-party risk to the exchange users. 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. In the meantime, a timelock-based mechanism can also be considered as mitigation.

Recommendation Promptly transfer the privileged account to the intended DAO-like governance contract. All changed 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 with a multi-sig account to take the role of the manager.

4 Conclusion

In this audit, we have analyzed the design and implementation of the staking reward contract in `UXLINK`, which aims to be the largest `Web3` social platform and infrastructure for users and developers to discover, distribute, and trade crypto assets in unique social and group-based manner. This audit focuses on the staking contract to reward staking users. During the audit, we notice that the current code base is well organized and those identified issues are promptly confirmed and fixed.

Meanwhile, we need to emphasize that 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.