SMART CONTRACT AUDIT REPORT

for

Lottery (ZKasino)

Prepared By: Xiaomi Huang

PeckShield

December 29, 2023

Document Properties

Client	ZKasino
Title	Smart Contract Audit Report
Target	ZKasino
Version	1.0
Author	Xuxian Jiang
Auditors	Jason Shen, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	December 29, 2023	Xuxian Jiang	Final Release
1.0-rc	December 28, 2023	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 smart contract source code of the `Lottery` contract in `ZKasino`, 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 ZKasino

`ZKasino` is a decentralised, crypto betting platform and blockchain casino. It aims to be the most fair and transparent platform with the lowest house edge compared to all other betting platforms. In the audited `Lottery` contract, players can buy tickets and at the end of the month the winner gets drawn with `Chainlink VRF`. A certain percentage of the pot goes to the winner, another to rebates (early ticket buyers), another to charity, another to the bankroll (as a fee) and another to the next round lottery. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of ZKasino

Item	Description
Name	ZKasino
Website	https://play.zkasino.io/
Type	Solidity Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	December 29, 2023

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

- https://github.com/zkasino/contracts.git (68f9139)

And this is the Git repository and commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/zkasino/contracts.git (a326bce)

1.2 About PeckShield

PeckShield Inc. [9] 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 [8]:

- 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) [7], 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 design and implementation of the `Lottery` support in `ZKasino`. 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 logic, 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	0	
Low	3	■■■
Informational	0	
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 3 low-severity vulnerabilities.

Table 2.1: Key ZKasino Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Revisited Lottery Prize Donation Logic in Lottery	Business Logic	Resolved
PVE-002	Low	Improved Ticket Rescue Logic in rescueTicket()	Coding Practices	Resolved
PVE-003	Low	Trust Issue of Admin Keys	Security Features	Resolved

Beside the identified issues, we emphasize that for any user-facing applications and services, 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 should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 Detailed Results

3.1 Revisited Lottery Prize Donation Logic in Lottery

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `Lottery`
- Category: Business Logic [6]
- CWE subcategory: CWE-841 [3]

Description

The `Lottery` contract allows user donation to increase the lottery prize. In particular, it accepts any user for the donation regardless whether the lottery is stopped, cancelled, or in an error state.

In the following, we show the implementation of the related `increaseLotteryPrize()` routine. It simply validates the given amount and then adds the amount to the winner pool. However, it should take the donation only when the lottery is in the `LotteryStatus.OPEN` state.

```
    function increaseLotteryPrize() external payable {
        if (msg.value == 0) {
            revert();
        }
        games[currentGameId].winnerPool += msg.value;
    }
```

Listing 3.1: `Lottery::increaseLotteryPrize()`

Recommendation Revise the above routine to ensure the donation can only be taken when the lottery is being open.

Status The issue has been fixed by this commit: `a326bce`.

3.2 Improved Ticket Rescue Logic in rescueTicket()

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `Lottery`
- Category: Coding Practices [5]
- CWE subcategory: CWE-563 [2]

Description

The `Lottery` contract allows users to withdraw betting funds when the lottery is cancelled or in an error state. While examining the current rescue logic, we notice it can be improved by deleting the user's `playerStats` storage state as well.

To elaborate, we show below the related routine `rescueTicket()`, which has a rather straightforward logic in returning the user funds. However, the remaining user-betting state is still saved in `playerStats`, which can be safely removed. In other words, we suggest to add the following statement upon the user fund return: `delete playerStats[t.player];`.

```
    function rescueTicket(uint256 ticketIndex) external nonReentrant {
        if (
            !(currentLotteryStatus == LotteryStatus.ERROR
                currentLotteryStatus == LotteryStatus.CANCELED)
        ) {
            revert InvalidLotteryState(
                currentLotteryStatus,
                LotteryStatus.ERROR
            );
        }

        Ticket memory t = games[currentGameId].tickets[ticketIndex];
        delete (games[currentGameId].tickets[ticketIndex]);
        uint256 totalValue = (1 + t.endIndex - t.startIndex) * TICKET_COST;
        _transferETH(t.player, totalValue);
    }
```

Listing 3.2: `Lottery::rescueTicket()`

Recommendation Revise the above routine to remove remaining user state in `playerStats`.

Status The issue has been fixed by this commit: `a326bce`.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `Lottery`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [1]

Description

In the `Lottery` contract, there is a privileged `owner` account that plays a critical role in governing and regulating the contract-wide operations (e.g., donate/rescue funds and cancel the lottery). In the following, we show the representative functions potentially affected by the privilege of the account.

```
    function closeLottery() external {
        if (msg.sender != IBankRoll(bankRoll).getOwner()) {
            revert();
        }
        stopLottery = true;
    }

    /**
     * @dev function to donate part of the funds belonging to the charity pot to any
         given address.
     * This function can only be called by the manager of the zkasino bankroll.
     * @param to address to send ETH to
     * @param amount amount of ETH to send
     */
    function donate(address to, uint256 amount) external nonReentrant {
        if (msg.sender != IBankRoll(bankRoll).getOwner()) {
            revert();
        }
        if (charityFunds < amount) {
            revert();
        }
        charityFunds -= amount;
        _transferETH(to, amount);
        emit DonationPerformed(to, amount);
    }
```

Listing 3.3: Example Privileged Operations in `Lottery`

We emphasize that the privilege assignment may be necessary and consistent with the protocol design. However, it would be better if the privileged account is governed by a DAO-like structure. Note that a compromised account would allow the attacker to modify a number of sensitive system parameters, which directly undermines the assumption of the protocol design.

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 The issue has been confirmed by the team. The team intends to manage the admin keys with a multi-sig account and later `DAO` at token launch.

4 Conclusion

In this audit, we have analyzed the design and implementation of the `Lottery` contract in `ZKasino`, which is a decentralised, crypto betting platform and blockchain casino. In the audited `Lottery` contract, players can buy tickets and at the end of the month the winner gets drawn with `Chainlink VRF`. A certain percentage of the pot goes to the winner, another to rebates (early ticket buyers), another to charity, another to the bankroll (as a fee) and another to the next round lottery. 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-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.html.

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

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

[5] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

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

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

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

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