SMART CONTRACT AUDIT REPORT

for

Band VRF & Bridge

Prepared By: Xiaomi Huang

PeckShield

September 23, 2022

Document Properties

Client	Band Protocol
Title	Smart Contract Audit Report
Target	Band VRF & Bridge
Version	1.0
Author	Xuxian Jiang
Auditors	Shulin Bie, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	September 23, 2022	Xuxian Jiang	Final Release
1.0-rc	September 9, 2022	Shulin Bie	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 Band VRF & Bridge, 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 Band VRF & Bridge

Band Protocol is a cross-chain data oracle aggregating and connecting real-world data and APIs to smart contracts, which is built on top of BandChain, a Cosmos SDK-based blockchain designed to be compatible with most smart contract and blockchain development frameworks. In particular, the audited Band VRF is a Verifiable Random Function (VRF) protocol based on the BandChain, and the audited Band Bridge allows anyone who requested data from the Band Oracle to verify the validity of the result they received.

Table 1.1: Basic Information of The Band VRF & Bridge

Item	Description
Target	Band VRF & Bridge
Type	EVM Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	September 23, 2022

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

- https://github.com/bandprotocol/vrf-and-bridge-contracts.git (6dd421b)

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

- https://github.com/bandprotocol/vrf-and-bridge-contracts.git (62834d2)

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.

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

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

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 `Band VRF & Bridge` 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	1	■
Low	0	
Informational	2	■ ■
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 1 medium-severity vulnerability and 2 informational recommendations.

Table 2.1: Key Band VRF & Bridge Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Informational	Suggested Event Generation for Key Operations	Coding Practices	Confirmed
PVE-002	Informational	Inconsistency Between Implementation and Document	Coding Practices	Fixed
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 Suggested Event Generation for Key Operations

- ID: PVE-001
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: `Bridge/VRFLens`
- Category: Coding Practices [5]
- CWE subcategory: CWE-563 [2]

Description

In `Ethereum`, the `event` is an indispensable part of a contract and is mainly used to record a variety of runtime dynamics. In particular, when an `event` is emitted, it stores the arguments passed in transaction logs and these logs are made accessible to external analytics and reporting tools. `Events` can be emitted in a number of scenarios. One particular case is when system-wide parameters or settings are being changed. Another case is when tokens are being minted, transferred, or burned.

While examining the events that reflect the protocol dynamics, we notice there are several key operations that lack meaningful events to reflect their changes. In the following, we show several representative routines.

```
function updateValidatorPowers(ValidatorWithPower[] calldata validators, uint256 expectedTotalPower)
    external
    onlyOwner
{
    uint256 _totalValidatorPower = totalValidatorPower;

    ...

    require(_totalValidatorPower == expectedTotalPower, "TOTAL_POWER_CHECKING_FAIL");
    totalValidatorPower = _totalValidatorPower;
}


```

```
    function relayBlock(
        MultiStore.Data calldata multiStore,
        BlockHeaderMerkleParts.Data calldata merkleParts,
        CommonEncodedVotePart.Data calldata commonEncodedVotePart,
        TMSignature.Data[] calldata signatures
    ) public {
        if (
            blockDetails[merkleParts.height].oracleState == multiStore.oracleIAVLStateHash &&
            blockDetails[merkleParts.height].timeSecond == merkleParts.timeSecond &&
            blockDetails[merkleParts.height].timeNanoSecondFraction == merkleParts.timeNanoSecondFraction
        ) return;

        ...

        blockDetails[merkleParts.height] = BlockDetail({
            oracleState: multiStore.oracleIAVLStateHash,
            timeSecond: merkleParts.timeSecond,
            timeNanoSecondFraction: merkleParts.timeNanoSecondFraction
        });
    }
```

Listing 3.1: `Bridge`

With that, we suggest to emit meaningful events for these key operations. Also, the key event information is better `indexed`. Note each emitted event is represented as a topic that usually consists of the signature (from a `keccak256` hash) of the event name and the types (`uint256`, `string`, etc.) of its parameters. Each indexed type will be treated like an additional topic. If an argument is not indexed, it will be attached as data (instead of a separate topic). Considering that the key information is typically queried, it is better treated as a topic, hence the need of being `indexed`.

Recommendation Properly emit the above-mentioned events with accurate information to timely reflect state changes. This is very helpful for external analytics and reporting tools.

Status The issue has been confirmed by the team.

3.2 Inconsistency Between Implementation and Document

- ID: PVE-002
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: `MultiStore`
- Category: Business Logic [6]
- CWE subcategory: CWE-841 [3]

Description

In the `Band Bridge` implementation, the `MultiStore` library is designed to calculate the `Tendermint`'s application state hash. In particular, the `getAppHash()` routine is used to calculate the application state hash according to the `Merkle Tree` shown below. While examining its logic, we notice there is a misleading comment embedded inside its implementation, which brings unnecessary hurdles to understand and/or maintain the software.

To elaborate, we show below the related code snippet of the `MultiStore` contract. By design, the `authToFeeGrantStoresMerkleHash` member of the `struct Data` represents `I12` of the `Merkle Tree`. However, inside the `getAppHash()` routine, it is annotated as `I10` (line 41). It will bring unnecessary hurdles to understand the design.

```
                                            ______________[AppHash]_______________
                                           /                                      \
                        _________________[I14]_________________                  [G]
                       /                                       \
           _______[I12]______                              _______[I13]_______
          /                  \                            /                   \
     __[I8]__             __[I9]__                  __[I10]__             __[I11]__
    /        \           /        \                /         \           /         \
  [I0]      [I1]       [I2]       [I3]          [I4]       [I5]       [I6]       [I7]
 /   \     /   \      /    \     /    \        /    \     /   \      /    \     /    \
[0]   [1] [2]   [3]  [4]    [5] [6]    [7]    [8]    [9] [A]   [B] [C]    [D] [E]    [F]
[0] - auth     [1] - authz    [2] - bank     [3] - capability [4] - crisis   [5] - dist
[6] - evidence [7] - feegrant [8] - gov      [9] - ibccore    [A] - mint     [B] - oracle
[C] - params   [D] - slashing [E] - staking  [F] - transfer   [G] - upgrade
```

Listing 3.2: Merkle Tree of Tendermint's Application State

```
27    library MultiStore {
28        struct Data {
29            bytes32 authToFeeGrantStoresMerkleHash; // [I12]
30            bytes32 govToIbcCoreStoresMerkleHash; // [I4]
31            bytes32 mintStoreMerkleHash; // [A]
32            bytes32 oracleIAVLStateHash; // [B]
33            bytes32 paramsToTransferStoresMerkleHash; // [I11]
34            bytes32 upgradeStoreMerkleHash; // [G]
35        }
```

```
    function getAppHash(Data memory self) internal pure returns (bytes32) {
        return
            Utils.merkleInnerHash( // [AppHash]
                Utils.merkleInnerHash( // [I14]
                    self.authToFeeGrantStoresMerkleHash, // [I10]
                    ...
                ),
                self.upgradeStoreMerkleHash // [G]
            );
    }
}
```

Listing 3.3: `MultiStore`

Recommendation Ensure the consistency between documents (including embedded comments) and implementation.

Status The issue has been addressed by the following commit: `d6b5152`.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Bridge/VRFProviderBase`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [1]

Description

In the `Band VRF & Bridge` implementation, there is a privileged `owner` account that plays a critical role in governing and regulating the protocol-wide operations (e.g., configuring system parameters and managing the privileged `validators`). In the following, we show the representative functions potentially affected by the privilege of the account.

```
function updateValidatorPowers(ValidatorWithPower[] calldata validators, uint256 expectedTotalPower)
    external
    onlyOwner
{
    uint256 _totalValidatorPower = totalValidatorPower;
    for (uint256 idx = 0; idx < validators.length; ++idx) {
        ValidatorWithPower memory validator = validators[idx];
        (bool found, uint256 oldPower) = validatorPowers.tryGet(validator.addr);
        if (found) {
            _totalValidatorPower -= oldPower;
        }
```

```

            if (validator.power > 0) {
                validatorPowers.set(validator.addr, validator.power);
                _totalValidatorPower += validator.power;
            } else {
                validatorPowers.remove(validator.addr);
            }
        }

        require(_totalValidatorPower == expectedTotalPower, "TOTAL_POWER_CHECKING_FAIL");
        totalValidatorPower = _totalValidatorPower;
    }
```

Listing 3.4: `Bridge::updateValidatorPowers()`

```
    function setBridge(IBridge _bridge) external onlyOwner {
        bridge = _bridge;
        emit SetBridge(address(_bridge));
    }
```

Listing 3.5: `VRFProviderBase::setBridge()`

We emphasize that the privilege assignment may be necessary and consistent with the protocol design. However, it is worrisome if the privileged account is not 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 privileged account will be managed by a multi-sig account.

4 Conclusion

In this audit, we have analyzed the `Band VRF & Bridge` design and implementation. `Band Protocol` is a cross-chain data oracle aggregating and connecting real-world data and APIs to smart contracts, which is built on top of `BandChain`, a `Cosmos SDK`-based blockchain designed to be compatible with most smart contract and blockchain development frameworks. In particular, the audited `Band VRF` is a `Verifiable Random Function` (`VRF`) protocol based on the `BandChain`, and the audited `Band Bridge` allows anyone who requested data from the `Band Oracle` to verify the validity of the result they received. The current code base is clearly organized and those identified issues are promptly confirmed and fixed.

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-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.