BLOCKSEC

Security Audit

Report for share-card Contracts

Date: July 10, 2026 **Version:** 1.0

Contact: contact@blocksec.com

Contents

Report Manifest

Item	Description
Client	Bitget
Target	share-card Contracts

Version History

Version	Date	Description
1.0	July 10, 2026	First release

Signature

Digitally signed by: BlockSec (https://blocksec.com)

SHA1 digest of public key: BAB106D3708BC6DE0963CE05E9478C24B326AE1C

Date: 2026-07-10 11:40:40+0000

About BlockSec BlockSec focuses on the security of the blockchain ecosystem and collaborates with leading DeFi projects to secure their products. BlockSec is founded by top-notch security researchers and experienced experts from both academia and industry. They have published multiple blockchain security papers in prestigious conferences, reported several zero-day attacks of DeFi applications, and successfully protected digital assets that are worth more than 14 million dollars by blocking multiple attacks. They can be reached at Email, Twitter and Medium.

Chapter 1 Introduction

1.1 About the Audit Target

Information	Description
Type	Smart Contract
Language	Solidity
Approach	Semi-automatic and manual verification

The audit target (hereinafter referred to as the Target) of this audit is the code repository [1] of share-card Contracts of Bitget.

The share-card Contracts of Bitget is a treasury system that manages asset deposits, releases, and refunds. Specifically, users can deposit assets (i.e., the defined payment token) via the function `deposit()` of the contract `CardTreasuryCore` and the asset will be held by the contract `CardTreasuryPool`. As for asset releases and refunds, only the roles `releaseExecutor` and `refundExecutor` are allowed to perform such operations based on users' valid signatures.

Note this audit focuses on the smart contracts located in the contracts directory, excluding the following directories/files:

- contracts/interfaces

Other files are not within the scope of the audit. Additionally, all dependencies of the Target are considered reliable in terms of both functionality and security, and are therefore not included in the audit scope.

The auditing process is iterative. Specifically, we would audit the commits that fix the discovered issues. If there are new issues, we will continue this process. The commit SHA values during the audit are shown in the following table. Our audit report is responsible for the code in the initial version (`Version 1`), as well as new code (in the following versions) to fix issues in the audit report. Code prior to and including the baseline version (`Version 0`), where applicable, is outside the scope of this audit and assumes to be reliable and secure.

Project	Version	Commit Hash
share-card	`Version 1`	`d62dbd245d7fe2337d7a0c3b14cd7b73a13875b5`
	`Version 2`	`99e7865521aeecf1d4abdedc0c46c137b2b25cd9`

1.2 Disclaimer

This 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.

[1] https://github.com/bitgetwallet/share-card

This 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 Target, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit cannot be considered comprehensive, we always recommend proceeding with independent audits and a public bug bounty program to ensure the security of the Target.

The scope of this audit is limited to the code mentioned in Section 1.1. 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.

1.3 Procedure of Auditing

We perform the audit according to the following procedure.

- **Vulnerability Detection** We first scan the Target with automatic code analyzers, and then manually verify (reject or confirm) the issues reported by them.
- **Semantic Analysis** We study the business logic of the Target and conduct further investigation on the possible vulnerabilities using an automatic fuzzing tool (developed by our research team). We also manually analyze possible attack scenarios with independent auditors to cross-check the result.
- **Recommendation** We provide some useful advice to developers from the perspective of good programming practice, including gas optimization, code style, and etc.

We show the main concrete checkpoints in the following.

1.3.1 Security Issues

* Access control
* Permission management
* Whitelist and blacklist mechanisms
* Initialization consistency
* Improper use of the proxy system
* Reentrancy
* Denial of Service (DoS)
* Untrusted external call and control flow
* Exception handling
* Data handling and flow
* Events operation
* Error-prone randomness
* Oracle security
* Business logic correctness
* Semantic and functional consistency
* Emergency mechanism
* Economic and incentive impact

1.3.2 Additional Recommendation

* Gas optimization
* Code quality and style

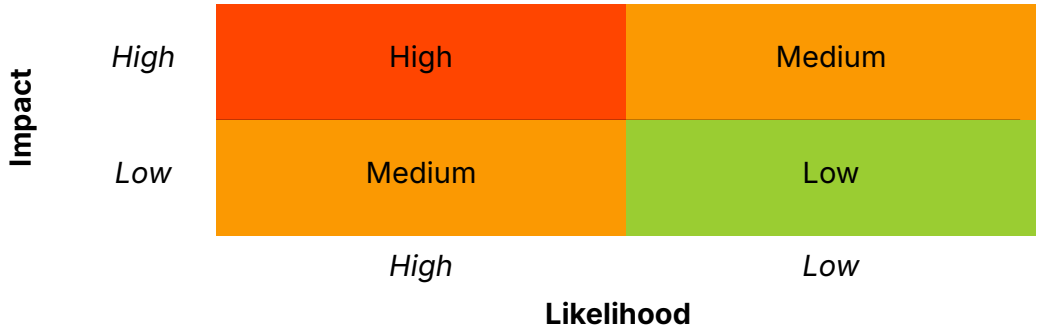
Note *The previous checkpoints are the main ones. We may use more checkpoints during the auditing process according to the functionality of the project.*

1.4 Security Model

To evaluate the risk, we follow the standards or suggestions that are widely adopted by both industry and academy, including OWASP Risk Rating Methodology [2] and Common Weakness Enumeration [3]. The overall *severity* of the risk is determined by *likelihood* and *impact*. Specifically, likelihood is used to estimate how likely a particular vulnerability can be uncovered and exploited by an attacker, while impact is used to measure the consequences of a successful exploit.

In this report, both likelihood and impact are categorized into two ratings, i.e., *high* and *low* respectively, and their combinations are shown in Table 1.1.

Table 1.1: Vulnerability Severity Classification



Accordingly, the severity measured in this report are classified into three categories: **High**, **Medium**, **Low**. For the sake of completeness, **Undetermined** is also used to cover circumstances when the risk cannot be well determined.

Furthermore, the status of a discovered item will fall into one of the following five categories:

- **Undetermined** No response yet.
- **Acknowledged** The item has been received by the client, but not confirmed yet.
- **Confirmed** The item has been recognized by the client, but not fixed yet.
- **Partially Fixed** The item has been confirmed and partially fixed by the client.
- **Fixed** The item has been confirmed and fixed by the client.

[2] https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

[3] https://cwe.mitre.org/

Chapter 2 Findings

In total, we have **two** recommendations and **two** notes.

- Recommendation: 2
- Note: 2

ID	Severity	Description	Category	Status
1	-	Remove redundant code	Recommendation	Confirmed
2	-	Use a proper error in the function `refund()`	Recommendation	Fixed
3	-	Proper selection of payment tokens	Note	-
4	-	Potential centralization risks	Note	-

The details are provided in the following sections.

2.1 Recommendation

2.1.1 Remove redundant code

Status Confirmed

Introduced by `Version 1`

Description In the contract `CardTreasuryBase`, the function `rescueETH()` is redundant. It is recommended to remove it for better code readability.

```
56   function rescueETH() external virtual override onlyOperator nonReentrant {
57       address _safe = safe;
58       if (_safe == address(0)) revert SafeNotSet();
59       uint256 amount = address(this).balance;
60       if (amount == 0) revert NothingToRescue();
61       TokenHelper.safeTransferETH(_safe, amount);
62       emit ETHRescued(amount, _safe, msg.sender);
63   }
```

Listing 2.1: contracts/CardTreasuryBase.sol

Suggestion Remove the redundant code.

2.1.2 Use a proper error in the function `refund()`

Status Fixed in `Version 2`

Introduced by `Version 1`

Description In the contract `CardTreasuryCore`, the function `refund()` reuses the `ExceedsReleasable` error for the check `totalNetDeposited - amount >= totalGlobalReleased`, which is semantically different from its use in the function `globalRelease()`. This mismatch makes on-chain revert diagnosis ambiguous. It is recommended to use a proper error in the function `refund()`.

```
69        if (params.amount > releasable) revert ExceedsReleasable();
```

Listing 2.2: contracts/CardTreasuryCore.sol

```
111       if (totalNetDeposited - params.amount < totalGlobalReleased) revert ExceedsReleasable();
```

Listing 2.3: contracts/CardTreasuryCore.sol

Suggestion Use a proper error in the function `refund()`.

2.2 Note

2.2.1 Proper selection of payment tokens

Introduced by `Version 1`

Description The project must properly select payment tokens for correct accounting and functionality. Specifically, the adoption of non-standard ERC20 tokens may cause incorrect accounting, leading to potential losses and the adoption of USDT on Tron may lead to potential DoS, due to the use of the functions `safeTransfer()` and `safeTransferFrom()`.

```
43    function _rescueERC20Internal(address token) internal {
44        address _safe = safe;
45        if (_safe == address(0)) revert SafeNotSet();
46        uint256 amount = IERC20(token).balanceOf(address(this));
47        if (amount == 0) revert NothingToRescue();
48        TokenHelper.safeTransfer(token, _safe, amount);
49        emit ERC20Rescued(token, amount, _safe, msg.sender);
50    }
51
52    function rescueERC20(address token) external virtual override onlyOperator nonReentrant {
53        _rescueERC20Internal(token);
54    }
```

Listing 2.4: contracts/CardTreasuryBase.sol

```
43    function deposit(DepositParams calldata params) external override whenNotPaused nonReentrant {
44        address pool = _validateAndGetPool(params.amount, params.deadline);
45
46        bytes32 structHash = _depositStructHash(msg.sender, params);
47        _verifySigner(structHash, params.signature);
48        _consumeNonce(params.nonce);
49
50        netDeposited[msg.sender] += params.amount;
51        totalNetDeposited += params.amount;
52
53        TokenHelper.safeTransferFrom(address(paymentToken), msg.sender, pool, params.amount);
54        emit Deposited(msg.sender, params.amount);
55    }
```

Listing 2.5: contracts/CardTreasuryCore.sol

2.2.2 Potential centralization risks

Introduced by `Version 1`

Description In this project, several privileged roles (e.g., `owner`) can conduct sensitive operations, which introduces potential centralization risks. For example, the role `owner` can migrate assets to arbitrary pools. If the private keys of the privileged accounts are lost or maliciously exploited, it could pose a significant risk to the protocol.


BOOST WEB3 THROUGH NEXT-GENERATION SECURITY & USABILITY INNOVATIONS