SIXR Cricket

Security Assessment

CertiK Assessed on Sept 15th, 2025

CertiK Assessed on Sept 15th, 2025

SIXR Cricket

The security assessment was prepared by CertiK.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Jetton	TON (TON)	Manual Review, Static Analysis

LANGUAGE	TIMELINE
FunC	Preliminary comments published on 09/15/2025
	Final report published on 09/15/2025

Vulnerability Summary

6	5	0	1	0
Total Findings	Resolved	Partially Resolved	Acknowledged	Declined

0	Centralization		Centralization findings highlight privileged roles & functions and their capabilities, or instances where the project takes custody of users' assets.
0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
1	Major	1 Acknowledged	Major risks may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.
2	Medium	2 Resolved	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
2	Minor	2 Resolved	Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
1	Informational	1 Resolved	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | SIXR CRICKET

Summary

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

Findings

SIC-06 : Initial Token Distribution

SIC-01 : Bounced `op::internal_transfer` Message From `jetton-minter` Is Not Processed

SIC-02 : `jetton-minter::op::mint` Allows To Send Invalid Messages

SIC-03 : `end_parse()` Is Missing

SIC-04 : Mutable Metadata In Jetton Smart Contract

SIC-05 : Unused Declarations

Appendix

Disclaimer

CODEBASE | SIXR CRICKET

Repository

According to the audited codebase, the contract was deployed at EQAqucy1Vv1yU3SPTwZOYiSShefgLT-9KRRW6x-GHrwgTlSH.

Commit

92c6a5caeafa87b3b79efd658053fd9b77b1b035

AUDIT SCOPE | SIXR CRICKET

CertiKProject/certik-audit-projects

- jetton-wallet.fc

Liberty-Games/Jetton

- import/constants.fc
- import/discovery-params.fc
- import/jetton-utils.fc
- import/op-codes.fc
- import/params.fc
- import/stdlib.fc
- import/utils.fc
- jetton-minter.fc

APPROACH & METHODS | SIXR CRICKET

This audit was conducted for SIXR Cricket to evaluate the security and correctness of the smart contracts associated with the SIXR Cricket project. The assessment included a comprehensive review of the in-scope smart contracts. The audit was performed using a combination of Manual Review and Static Analysis.

The review process emphasized the following areas:

- Architecture review and threat modeling to understand systemic risks and identify design-level flaws.
- Identification of vulnerabilities through both common and edge-case attack vectors.
- Manual verification of contract logic to ensure alignment with intended design and business requirements.
- Dynamic testing to validate runtime behavior and assess execution risks.
- Assessment of code quality and maintainability, including adherence to current best practices and industry standards.

The audit resulted in findings categorized across multiple severity levels, from informational to critical. To enhance the project's security and long-term robustness, we recommend addressing the identified issues and considering the following general improvements:

- Improve code readability and maintainability by adopting a clean architectural pattern and modular design.
- Strengthen testing coverage, including unit and integration tests for key functionalities and edge cases.
- Maintain meaningful inline comments and documentations.
- Implement clear and transparent documentation for privileged roles and sensitive protocol operations.
- Regularly review and simulate contract behavior against newly emerging attack vectors.

FINDINGS | SIXR CRICKET

6	0	0	1	2	2	1
Total Findings	Critical	Centralization	Major	Medium	Minor	Informational

This report has been prepared for SIXR Cricket to identify potential vulnerabilities and security issues within the reviewed codebase. During the course of the audit, a total of 6 issues were identified. Leveraging a combination of Manual Review & Static Analysis the following findings were uncovered:

ID	Title	Category	Severity	Status
SIC-06	**Initial Token Distribution**	**Centralization**	**Major**	**Acknowledged**
SIC-01	Bounced `op::internal_transfer` Message From `jetton-minter` Is Not Processed	Inconsistency	Medium	Resolved
SIC-02	`jetton-minter::op::mint` Allows To Send Invalid Messages	Logical Issue	Medium	Resolved
SIC-03	`end_parse()` Is Missing	Coding Style	Minor	Resolved
SIC-04	Mutable Metadata In Jetton Smart Contract	Volatile Code	Minor	Resolved
SIC-05	Unused Declarations	Coding Style	Informational	Resolved

SIC-06 | Initial Token Distribution

Category	Severity	Location	Status
Centralization	**Major**		**Acknowledged**

Description

All of the SIXR tokens were minted to one address UQAOsCLGJ4hWKJv3O_vSuwTihRAnBXtOFJmaWVdRZFBZKdGv. This poses a significant centralization risk as this one entity controls all the supply. Such centralization can lead to market manipulation, reduced trust, and potential governance issues within the network. Decentralization is key to maintaining a secure and resilient blockchain ecosystem.

Recommendation

It's recommended the team be transparent regarding the initial token distribution process. The token distribution plan should be published in a public location that the community can access. The team shall make enough efforts to restrict the access of the private keys. A multi-signature (⅔, ⅗) wallet can be used to prevent a single point of failure due to the private key compromise. Additionally, the team can lock up a portion of tokens, release them with a vesting schedule for long-term success, and deanonymize project teams with a third-party KYC provider to create greater accountability.

Alleviation

[SIXR Cricket, 09/14/2025]: The token will be distributed using vesting services like sablier and locked up according to the tokeneconomy before the TGE.

Category	% Percentage	Token Allocatic	Price	Amount to Ra	Clif	Vesti	TGE U	TGE Token
Liberty Games	20%	200.000.000,00	-	-	6	24	1%	2.000.000
Advisors	5%	50.000.000,00	-	-	12	24	2,5%	1.250.000
Ecosystem Development	3%	30.000.000,00	-	-	3	24	0%	0
Affiliates	1,5%	15.000.000,00	-	-	6	18	0%	0
Marketing	4%	40.000.000,00	-	-	12	24	2,5%	1.000.000
Ambassadors/Players	3%	30.000.000,00	-	-	12	20	0%	0
Game Rewards	12%	120.000.000,00	-	-	0	24	2,5%	3.000.000
Staking Rewards	5%	50.000.000,00	-	-	3	24	0%	0
Community Funding	6%	60.000.000,00	-	-	10	16	0%	0
Team	5%	50.000.000,00	-	-	6	24	5%	2.500.000
Liquidity/MM/Exchanges	8%	80.000.000,00	-	-	0	0	100%	80.000.000
Seed Round	0,5%	5.000.000,00	0,010 €	50.000,000 €	12	30	5%	250.000
Extended Seed Round	5%	50.000.000,00	0,020 €	1.000.000,000 €	8	24	10%	5.000.000
Private Round 1	2%	20.000.000,00	0,025 €	500.000,000 €	7	20	10%	2.000.000
Private Round 2	5%	50.000.000,00	0,030 €	1.500.000,000 €	7	18	10%	5.000.000
Private Round 3	11%	110.000.000,00	0,045 €	4.950.000,000 €	6	18	10%	11.000.000
Public Round	4%	40.000.000,00	0,050 €	2.000.000,000 €	3	9	25%	10.000.000

SIC-01 Bounced `op::internal_transfer` Message From `jetton-minter` Is Not Processed

Category	Severity	Location	Status
Inconsistency	Medium	jetton-minter.fc (jetton): 79~80	Resolved

Description

When the `op::internal_transfer` message is bounced from one `jetton-wallet` to another one, the `balance` is updated (increased back).

However, if the `op::internal_transfer` message is bounced from `jetton-wallet` to `jetton-minter`, the `total_supply` is not updated.

`master_msg` provided to `op::mint` is not validated and passed as is to `jetton-wallet`. Cell underflow can happen.

As a result, the total circulating supply will be less than `total_supply`.

Recommendation

We recommend handling properly the bounced messages in `jetton-minter`. We recommend validating the `master_msg` and the `amount` to be accepted by `jetton-wallet`.

Alleviation

Since the `admin` role was renounced, the issue is considered resolved.

SIC-02 | `jetton-minter::op::mint` Allows To Send Invalid Messages

Category	Severity	Location	Status
Logical Issue	Medium	jetton-minter.fc (jetton): 76~77	Resolved

Description

```
 70      if (op == op::mint()) {
 71          throw_unless(73, equal_slices(sender_address, admin_address));
 72          slice to_address = in_msg_body~load_msg_addr();
 73          int amount = in_msg_body~load_coins();
 74          cell master_msg = in_msg_body~load_ref();
 75          slice master_msg_cs = master_msg.begin_parse();
 76          master_msg_cs~skip_bits(32 + 64); ;; op + query_id
 77          int jetton_amount = master_msg_cs~load_coins();
 78          mint_tokens(to_address, jetton_wallet_code, amount, master_msg);
 79          save_data(total_supply + jetton_amount, admin_address, content,
jetton_wallet_code);
```

`jetton-minter::op::mint` is supposed to allow `admin_address` to mint new jettons to `to_address` via sending of `op::internal_transfer` message. However, `master_msg` is not validated:

- any `op` can be used
- the `op::internal_transfer` message format is not validated
- the `forward_ton_amount` argument is not respected, `min_tons_for_storage` is not provided
- `msg_value` is not controlled, `CARRY_REMAINING_GAS` mode is not used
- the bounced message is not handled, `total_supply` is not decreased back in case of failure

Recommendation

We recommend checking all the required arguments of `op::internal_transfer` message, we recommend handling of bounced message.

Alleviation

Since the `admin` role was renounced, the issue is considered resolved.

SIC-03 | `end_parse()` Is Missing

Category	Severity	Location	Status
Coding Style	Minor	jetton-minter.fc (jetton): 16; jetton-wallet.fc (jetton): 32	Resolved

Description

The data is packed in slice and parsed by the contract. To ensure the slice has the expected data structure and no data left after parsing, `end_parse()` can be applied to the slice. If slice is not empty, it throws an exception.

Recommendation

We recommend calling `end_parse()` to ensure the slice doesn't contain more data.

Alleviation

The absence of `end_parse()` is an issue inherent in the original TON Jetton contract. Therefore, we consider this finding to be non-exploitable and have Resolved it accordingly.

SIC-04 | Mutable Metadata In Jetton Smart Contract

Category	Severity	Location	Status
Volatile Code	Minor	jetton-minter.fc (jetton): 138~141	Resolved

Description

```
138     if (op == 4) { ;; change content, delete this for immutable tokens
139         throw_unless(73, equal_slices(sender_address, admin_address));
140         save_data(total_supply, admin_address, in_msg_body~load_ref(),
jetton_wallet_code);
141         return ();
142     }
```

The jetton-minter smart contract contains functionality that allows the metadata (such as token name, decimals, description, etc.) to be altered after deployment. This poses a significant security risk, as malicious actors could exploit this feature to mislead users, manipulate token properties, or cause other unpredictable behaviors.

Recommendation

We recommend removing of `op == 4` that allows changes to jetton metadata. Ensure that once the contract is deployed, the metadata remains constant to maintain trust and integrity in the token.

Alleviation

Since the `admin` role was renounced, the issue is considered resolved.

SIC-05 | Unused Declarations

Category	Severity	Location	Status
Coding Style	Informational	imports/constants.fc (jetton): 1~13; imports/utils.fc (jetton): 1	Resolved

Description

Constant declarations in constans.fc are not used, except `const::provide_address_gas_consumption`. `send_grams()` in utils.fc is never used.

Recommendation

We recommend removing of unused functionality.

Alleviation

These declarations are remnants of the original code and do not affect the contract's operation or security. Therefore, we consider this finding to be non-exploitable and have Resolved it accordingly.

APPENDIX | SIXR CRICKET

Finding Categories

Categories	Description
Coding Style	Coding Style findings may not affect code behavior, but indicate areas where coding practices can be improved to make the code more understandable and maintainable.
Inconsistency	Inconsistency findings refer to different parts of code that are not consistent or code that does not behave according to its specification.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases and may result in vulnerabilities.
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.

DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Elevating Your Web3 Journey

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is the largest blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.