InterBridge
Audit Report

Thu Oct 17 2024

✉ contact@bitslab.xyz https://twitter.com/tonbit_

TonBit

InterBridge Audit Report

1 Executive Summary

1.1 Project Information

Description	InterBridge is a liquidity pool-based bridge that allows users to add liquidity on Solana and TON. Users lock tokens on one chain, and InterBridge's infrastructure releases corresponding tokens to the users on the other chain.
Type	Bridge
Auditors	TonBit
Timeline	Wed Oct 02 2024 - Tue Oct 15 2024
Languages	Typescript
Platform	Ton,Solana
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/soonlabs/cross-chain-bridge-relayer https://github.com/soonlabs/cross-chain-bridge-data-sync
Commits	https://github.com/soonlabs/cross-chain-bridge-relayer: bf2d541de61c02ac26e9d08ce4b4af5487429e88 ef26ecf8c7ff34707e120213ef8537836c09d10b https://github.com/soonlabs/cross-chain-bridge-data-sync: 357b7149d0834b1ffaa5437d939b9c3123efc7a4 afb16098c2745edfe3e1942a31d15110cd669c36

1.2 Files in Scope

The following are the SHA1 hashes of the original reviewed files.

ID	File	SHA-1 Hash
LRU	contracts/bridge_gate/utils/liquidity_recorder_utils.fc	6ad9697a872c945a4c102e6e83c7db6608e1e226
UTI	contracts/bridge_gate/utils/utils.fc	1318fc037f1ae5665bf80b65886ab2b7ecc93da9
STO	contracts/bridge_gate/storage.fc	20eefa0ae64045548606fee644bbc5023ca0b5d8
CON	contracts/bridge_gate/constant.fc	2f059a17a5b1f66ffc2b7e8fd7b35074e39fa112
PAR	contracts/bridge_gate/params.fc	3e86ce82bee70992c9b0f7b4fcacf0cacfcfec1b
OPC	contracts/bridge_gate/opcode.fc	3f8028eedb23e4eb3398d461fb64d5c561179d7b
ECO	contracts/bridge_gate/error_codes.fc	9046b12637e4246b3d2c59ce631533c0af75a455
MES	contracts/bridge_gate/messages.fc	a20b0e0b0b61f709b49307d940d212d1d47cb8f3
GME	contracts/bridge_gate/get_method.fc	00009d4fb5b70c10fdf68c5d8f0cc5549a6cddd2
URO	contracts/bridge_gate/instructions/update_route.fc	2163e0cf74f5b5375ab9f1ce0f71ebe740859436
ALC	contracts/bridge_gate/instructions/add_liquidity_configuration.fc	54e057399a817c184ed2dbf3db655fa25877bc76

BOF	contracts/bridge_gate/instructions/bridge_out_ft.fc	57b9716547d88cb3ae40a73f0cfdfd17667e2b75
ARO	contracts/bridge_gate/instructions/add_route.fc	586d1128e74973618c93cc1166189080b615a4c1
UPG	contracts/bridge_gate/instructions/upgrade.fc	b34c1e2a5b9543bfd94c222fc0847c1a6f6a9727
ALF	contracts/bridge_gate/instructions/add_liquidity_ft.fc	962b466d5ff79298cba1fe11262cb0e10d429aec
BOT	contracts/bridge_gate/instructions/bridge_out_ton.fc	a81f2ffbf47af70474d9b27ff7e51d3448944f0c
REB	contracts/bridge_gate/instructions/relayer_execute_bridge.fc	70929198bd8d7b215a3c671363c74260cb2bcaf4
URE	contracts/bridge_gate/instructions/update_relayer.fc	1add49cd49d58bc843604bfd62b5c2816e79fa33
WLI	contracts/bridge_gate/instructions/withdraw_liquidity.fc	835c8013365292e11638946a528a1a0888a26ac9
ULC	contracts/bridge_gate/instructions/update_liquidity_configuration.fc	261a09ea9c89bc853b144dc94ec81bcb85eda1ae
ALT	contracts/bridge_gate/instructions/add_liquidity_ton.fc	dccf747aad71dc9464f68b78ca7139a47975fd73
LRE	contracts/liquidity_recorder.fc	19c34de21a485778c4948a6be009a8e5614de22d
LRU1	contracts/liquidity_recorder/utils/liquidity_recorder_utils.fc	84c9c54925c60cdbf6b92068918e4f2570a02824
STO1	contracts/liquidity_recorder/storage.fc	257412d12c1188d316645d50846588d2fe2bf8ba

CON1	contracts/liquidity_recorder/constant.fc	a94dfd9b7fe1810372228ad3c41cb27672b0cc7f
OPC1	contracts/liquidity_recorder/opcode.fc	7e47f9ee8968fd7b703024af4c48a0a8f8b90df6
ECO1	contracts/liquidity_recorder/error_codes.fc	cee17c0c64f7cbcbe2928b85fddeade25fdac136
MES1	contracts/liquidity_recorder/messages.fc	4a5aedeefce81ef2ae47a8597344ed7274abf16f
GME1	contracts/liquidity_recorder/get_method.fc	a6fc0af9de6eef075a78f87b02056adabf95887c
RLI	contracts/liquidity_recorder/instructions/recover_liquidity.fc	53abee32ffb783cdd12121ca95a07f796b5c94cc
WLI1	contracts/liquidity_recorder/instructions/withdraw_liquidity.fc	b52b33641cb2f79864897b010e38c4dc01c97a16
ALI	contracts/liquidity_recorder/instructions/add_liquidity.fc	7713c4ae65ac88289944979f0c852452379545d6
STD	contracts/jetton/stdlib.fc	48ba5be2230d6db462adb890e7b15ff0b36b90de
OCO	contracts/jetton/op-codes.fc	de6e2645c68d08535a353fa1b6bde7ac915d8ef5
DPA	contracts/jetton/discovery-params.fc	6809258270f1565706bba2eb7f3bcf5b2289e0ac
UTI1	contracts/jetton/utils.fc	19cd144cd1353e5179c9cefdd1e9b4f484f4b016
CON2	contracts/jetton/constants.fc	4630656a3a259560d0f49710829754698357f4d1

JUT	contracts/jetton/jetton-utils.fc	e725b3a317c7c347307c6c7a4b689119c04c8b58
STO2	contracts/ton_vault/storage.fc	6532614df08e4e0a9a81a05639e5af778bb90c0f
IUT	contracts/ton_vault/interface_utils.fc	9728876b81872ad4232fe346d19a6e458b2080e9
CON3	contracts/ton_vault/constant.fc	071d7be8f3a8973181593f01b988e11e1bba3a35
ECO2	contracts/ton_vault/error_codes.fc	19532807cd1bd8b2b9da0701877ea718f82fa51d
STD1	contracts/ton_vault/imports/stdlib.fc	2f104cd568a4cebb1c4112ecf8979800f0672575
MES2	contracts/ton_vault/messages.fc	a4f3f83c76803c5522938bc6e50d89b8b6425b4c
OPC2	contracts/ton_vault/opcodes.fc	5eaa009e31f77e038d3ccdb5d4ec1106fe5a9a6a
GME2	contracts/ton_vault/get_method.fc	794e103da83a697723f62e759f6a8adf94bf0e11
UTI2	contracts/ton_vault/utils.fc	796e0f1b0898879dfef264be2788a6bf529e4eda
TIN	contracts/ton_vault/instructions/transfer_in.fc	81b2b476a1f52cf0756861ce2362ccdf06c5d1bc
UPG1	contracts/ton_vault/instructions/upgrade.fc	28b383ff22ab72606b38b62b08d93934886303b2
TOU	contracts/ton_vault/instructions/transfer_out.fc	137d86ee3144e055a02d66d9d0344a37ded493e7

JWA	contracts/jetton-wallet.fc	3652a95818144d37e6f1be52a6c86ed41597ec5c
JMI	contracts/jetton-minter.fc	4bd79f928bfc9f8efdff363dca3a4d20e42f520f
CON4	contracts/common/constant.fc	d383ea70f2065a031fff856d6e3f6b97d86c774e
OPC3	contracts/common/opcode.fc	3a222564baf155a0f93ace862d171f90e3722a21
UTI3	contracts/common/utils.fc	8dd30e38723b7b4af03ae3a3b39ff9ab1589591e
TVA	contracts/ton_vault.fc	95d163161d610f32a8bbdf0f5a1831696739b2ed
BGA	contracts/bridge_gate.fc	c67bf0246fe2c6418f4e0436fcadcfd55a0ec921
ERR	programs/ton-bridge-program/src/errors.rs	1e9c294695772a428d76eac69256fbc72ddc9f9f
LIB	programs/ton-bridge-program/src/lib.rs	d0090bec108dc96cefb8c937f0be23961a7c5a04
BIN	programs/ton-bridge-program/src/states/bridge_intention.rs	894a7581d634aa8a3857282fcbcb5bb36bc1766b
BRO	programs/ton-bridge-program/src/states/bridge_route.rs	f1d9ea24e15d7b12e9c9e6715ff91687ea58c185
GCO	programs/ton-bridge-program/src/states/global_config.rs	c36a96489eebea741410d1195ad91d047faa8cda
MOD	programs/ton-bridge-program/src/states/mod.rs	9bd99c9427d88a7acacc0e7148c055413c3780c4

LIQ	programs/ton-bridge-program/src/states/liquidity.rs	371cec73e616223f78370017bbcd1a0a10a88df8
BRE	programs/ton-bridge-program/src/states/bridge_receipt.rs	0861e04f534e614f0e7cbd705a7d5af8479f41ef
PTBPSCMR	programs/ton-bridge-program/src/constants/mod.rs	9ef46f48a99805bbb276326ec8ce7755e6d5947d
RSL	programs/ton-bridge-program/src/instructions/remove_sol_liquidity.rs	b4f647ecfae048a8dcee6084ada2850ee5daab4b
WPF	programs/ton-bridge-program/src/instructions/withdraw_protocol_fee.rs	d3953f2c7f9c99b0ca84d58669cd296cf11825d4
TOTLW	programs/ton-bridge-program/src/instructions/turn_off_token_lp_whitelist.rs	37815b3a816aef1e3d4b55208e4bca6d85b128b3
PTBPSIRSLR	programs/ton-bridge-program/src/instructions/remove_spl_liquidity.rs	813dd3c4433435322b6aa6f4c1538bf6442c4727
BTD	programs/ton-bridge-program/src/instructions/bridge_to_destination.rs	949948c2ee99aeb0eb8a6e1a8ebd9de2ff1249b7
RRE	programs/ton-bridge-program/src/instructions/remove_relayer.rs	66bbd33cf1c552b7fd0192d6c66d857530240700
ASL	programs/ton-bridge-program/src/instructions/add_sol_liquidity.rs	ba8d73be796d444282ecacc4ef388ded89da3a42
PTBPSIASLR	programs/ton-bridge-program/src/instructions/add_spl_liquidity.rs	51687a4c1112020a6622fb0824dddd66c726a465
PBR	programs/ton-bridge-program/src/	c56a886355983a4b846b69dced2d

	instructions/pause_bridge_route.rs	c574a6219867
BFD	programs/ton-bridge-program/src/instructions/bridge_from_destination.rs	2e64f603d34369cc5da2987c0721b27975644c78
UBL	programs/ton-bridge-program/src/instructions/update_bridge_limit.rs	beff9caba02773d9fa3976230eb2b454c7f2ae26
UFF	programs/ton-bridge-program/src/instructions/update_fixed_fee.rs	ddcc4af277647fb37a84458226367d145829a9be
UAD	programs/ton-bridge-program/src/instructions/update_admin.rs	449aeb1f9d5f22bbf3b5e0ec2a8497579c8b9b10
ALWM	programs/ton-bridge-program/src/instructions/add_lp_whitelist_member.rs	75c3d3c46e817e50dbd2411a620470607161a314
ARE	programs/ton-bridge-program/src/instructions/add_relayer.rs	b62cf15fbbafd09c610514e069ee6b467f7fffe0
RLWM	programs/ton-bridge-program/src/instructions/remove_lp_whitelist_member.rs	13cb2aff8f3caa7781752bff8cb6e7acebcb94fc
PTBPSIMR	programs/ton-bridge-program/src/instructions/mod.rs	8fbffbf80b5355596988c6791fc6094f0545c9c0
IGC	programs/ton-bridge-program/src/instructions/initialize_global_configs.rs	697175afee912c8c85b6114352b267d4f2877c57
CBR	programs/ton-bridge-program/src/instructions/create_bridge_route.rs	8a88614b795e7c89da657b7026bb58e6e83fc52c
PTBPSITOTLWR	programs/ton-bridge-program/src/instructions/turn_on_token_lp_whitelist.rs	d2c2cd77c41a18e98d0b66588fb1e157d1ffa969

UBR	programs/ton-bridge-program/src/instructions/unpause_bridge_route.rs	bf6e2ff852fab4bd85b9a38342311229bf5fda9e
UFP	programs/ton-bridge-program/src/instructions/update_fee_percent.rs	015434640b0ed27682c9b7f2be9d48e440d7e9f2

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	7	6	1
Informational	1	1	0
Minor	0	0	0
Medium	2	1	1
Major	1	1	0
Critical	3	3	0

1.4 TonBit Audit Breakdown

TonBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow by bit operations
- Number of rounding errors
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting
- Unchecked CALL Return Values

1.5 Methodology

The security team adopted the **"Testing and Automated Analysis"**, **"Code Review"** strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

The code scope is illustrated in section 1.2.

(3) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by InterSOON to identify any potential issues and vulnerabilities in the source code of the InterBridge smart contract, as well as any contract dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we identified 7 issues of varying severity, listed below.

ID	Title	Severity	Status
ASL-1	Liquidity Provider Can Treat SOL as SPL When Adding SPL Liquidity	Critical	Fixed
BGA-1	Centralization Risk	Medium	Acknowledged
BOF-1	Redundant Calculation	Informational	Fixed
REB-1	Lack of Permission Check in `relayer_execute_bridge` Function	Major	Fixed
RSL-1	Conversion from u128 to u64 Type Leads to Loss of Funds	Critical	Fixed
TVA-1	Ton Vault Contract Cannot Be Upgraded	Medium	Fixed
RSL1-1	Liquidity Provider Can Treat SPL as SOL When Reducing SOL Liquidity	Critical	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the InterBridge Smart Contract :

Ton Contract:

1. Users on Ton call the contract for cross-chain operations.

2. Admin sets the contract parameters.

3. Relayer calls the contract to transfer funds from Solana.

Solana Contract:

1. Users on Solana call the contract for cross-chain operations.

2. Admin sets the contract parameters.

3. Relayer calls the contract to transfer funds from Ton.

User: Calls the contract on either Ton or Solana for cross-chain operations.

Admin: Sets contract parameters, LP whitelist, etc.

Relayer: Receives on-chain events from Ton or Solana and performs cross-chain operations.

LP: Liquidity Provider.

4 Findings

ASL-1 Liquidity Provider Can Treat SOL as SPL When Adding SPL Liquidity

Severity: Critical

Status: Fixed

Code Location:

programs/ton-bridge-program/src/instructions/add_sol_liquidity.rs#64

Descriptions:

In the `add_sol_liquidity` instruction, the LP provided `local_mint_key` parameter is not checked to see if it is SOL. If a `SPL` is more valuable than `SOL` ,a malicious LP could pass an `SPL Pubkey` to exchange for this more valuable SPL.

Suggestion:

1. Check if `local_mint_key` is SOL

BGA-1 Centralization Risk

Severity: Medium

Status: Acknowledged

Code Location:

contracts/bridge_gate.fc

Descriptions:

Centralization risk was identified in the smart contract.

- The admin can withdraw assets from the contract through the `withdraw_ton` function.
- The admin can upgrade the contract through the `upgrade` function.

Suggestion:

It is recommended to take ways to reduce the risk of centralization.

BOF-1 Redundant Calculation

Severity: Informational

Status: Fixed

Code Location:

contracts/bridge_gate/instructions/bridge_out_ft.fc#35

Descriptions:

In the `bridge_out_ft` function, the `calculate_hash_of_route` function is used to compute the r `oute_hash`, but this value is not used afterward. Instead, the `route_hash` is recalculated in the `load_router` function. We believe the calculation before `load_router` is redundant.

Suggestion:

It is recommended to remove the redundant calculation of `route_hash`.

REB-1 Lack of Permission Check in `relayer_execute_bridge` Function

Severity: Major

Status: Fixed

Code Location:

contracts/bridge_gate/instructions/relayer_execute_bridge.fc#11

Descriptions:

In the `relayer_execute_bridge` function, we found that the caller can extract assets from the vault to any specified address. Since this function lacks proper permission checks, it allows anyone to withdraw assets, which poses a significant security risk.

Suggestion:

It is recommended to add a permission check for the function.

RSL-1 Conversion from u128 to u64 Type Leads to Loss of Funds

Severity: Critical

Status: Fixed

Code Location:

programs/ton-bridge-program/src/instructions/remove_spl_liquidity.rs#69;

programs/ton-bridge-program/src/instructions/remove_sol_liquidity.rs#43;

programs/ton-bridge-program/src/instructions/add_sol_liquidity.rs#64;

programs/ton-bridge-program/src/instructions/add_spl_liquidity.rs#111

Descriptions:

In several places within the Solana contract, there are incorrect type conversions. For example, in `ton-bridge-program-/programs/ton-bridge-program/src/instructions/add_spl_liquidity.rs#111`, if an LP sets the amount to `(u128::MAX << 64) | 1`, the amount will be converted to u64 and equal to 1. This means the LP only transfers `1 SPL`, but the recorded amount in the ledger is `340282366920938463444927863358058659841 SPL`.

Suggestion:

1. Set the parameter type to u64
2. Or check if the u128 type parameter exceeds the maximum value of u64

TVA-1 Ton Vault Contract Cannot Be Upgraded

Severity: Medium

Status: Fixed

Code Location:

contracts/ton_vault.fc#40

Descriptions:

Based on the business logic of the `brigade_gate` contract, the `Ton vault` contract is invoked by the `brigade_gate` contract, specifically through functions like `transfer_in` and `transfer_out`. Both functions check the caller, indicating that the admin of the `Ton vault` contract is set to the address of the `brigade_gate` contract. Although the `brigade_gate` contract has an `upgrade` function, it only upgrades its own contract, and it seems that the `upgrade` function in the `Ton vault` is not invoked by `brigade_gate`. This could result in the `Ton vault` contract being unable to upgrade.

Suggestion:

It is recommended to confirm it aligns with your design.

RSL1-1 Liquidity Provider Can Treat SPL as SOL When Reducing SOL Liquidity

Severity: Critical

Status: Fixed

Code Location:

programs/ton-bridge-program/src/instructions/remove_sol_liquidity.rs#45

Descriptions:

In the `remove_sol_liquidity` instruction, the LP provided `local_mint_key` parameter is not checked to see if it is SOL. A malicious LP could pass an `SPL Pubkey` that is cheaper than `SOL` to exchange for the more valuable SOL.

Suggestion:

1. Check if `local_mint_key` is SOL

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed:** The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.

TONBIT VERIFIED