CKB-RGBppLock
Audit Report

Wed Jul 03 2024

contact@bitslab.xyz https://twitter.com/scalebit_

ScaleBit

CKB-RGBppLock Audit Report

1 Executive Summary

1.1 Project Information

Description	RGBpp-lock:A lock script that transfers cell ownership to a Bitcoin UTXO seal. BTCTimeLock:BTCTimeLock is a time lock used when an owner migrates RGB++ assets from Bitcoin to CKB. The assets must remain locked for at least six Bitcoin blocks to safeguard them against potential chain reorgs.
Type	Bitcoin & Asset Protocol
Auditors	ScaleBit
Timeline	Thu Jun 20 2024 - Tue Jul 02 2024
Languages	Rust
Platform	CKB
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/ckb-cell/rgbpp
Commits	83ce1589de9c8654bfe105afcbea760e6154dca6

1.2 Files in Scope

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

ID	File	SHA-1 Hash
LIB	crates/core/src/lib.rs	d53c4872cd5f4d4183898fdd93cd3d78eaed1d3e
BLC	crates/core/src/on_chain/bitcoin_light_client.rs	3c2df863e3563b949d40363dbb6c5c91311f4466
CCSOCMR	crates/core/src/on_chain/mod.rs	48637081147d0158767a74a3ec7dadf9340ff0f0
UTI	crates/core/src/on_chain/utils.rs	22c3383f60efaf1d3fe72169c998e7317ff5a33a
CCSRR	crates/core/src/rgbpp.rs	a6a2368498588a2d8ea0b579bd4745dc647c37a3
ERR	crates/core/src/error.rs	af4bc45dfb17d7bee5437e77b6c42420dde9f155
ENC	crates/core/src/bitcoin/encoder.rs	a5ff5d6dcea6bf0ee9d5356d1c1dea4c404ff4c5
PAR	crates/core/src/bitcoin/parser.rs	eb435e98d02a7217232142e0b5382158b3530910
TYP	crates/core/src/bitcoin/types.rs	1b7bf88c9392000515af7e2d4b038b3d37add2dc
CCSBMR	crates/core/src/bitcoin/mod.rs	07c7768c9f8ecbd8f2e1a40b58e552a75a3374a7
CCSBUR	crates/core/src/bitcoin/utils.rs	3e50b76f927e406178340898d0804e278f8eda19

CCSUR	crates/core/src/utils.rs	ab6674472b2245c70f72dbd3304f1c06295b8caa
MAI	contracts/btc-time-lock/src/main.rs	be843de8d430a03308883a41750e938e6fb52540
CRLSMR	contracts/rgbpp-lock/src/main.rs	b78ffcea060bcc733305a769194236e6df08940f

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	1	0	1
Informational	1	0	1
Minor	0	0	0
Medium	0	0	0
Major	0	0	0
Critical	0	0	0

1.4 ScaleBit Audit Breakdown

ScaleBit 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
- Number of rounding errors
- Unchecked CALL Return Values
- Functionality Checks
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic issues
- Replay attacks
- Coding style issues

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 CKB to identify any potential issues and vulnerabilities in the source code of the RGBppLock 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.

(1) Dependency Check

A comprehensive analysis of the software's dependency libraries was conducted using the Govulncheck tool.

(2) Automated Static Code Analysis

The code quality was examined using a code scanner.

During the audit, we identified 1 issues of varying severity, listed below.

ID	Title	Severity	Status
RGB-1	RGBpplock Cell Binding to Commitment	Informational	Acknowledged

3 Participant Process

Here are the relevant actors with their respective abilities within the RGBppLock Smart Contract :
RGBppLock is a CKB contract that utilises one-time sealing technology and SPV verification. Its key elements include

1. RGBppLock
2. BTC-Time-Lock

For RGBppLock as long as any CKB transaction that meets the contract verification requirements can be unlocked RGBppLock, the core logic of RGBppLock is one-time sealing, the user through BTC submits the relevant containment of the commitment of the transaction, in RGBppLock contract through certain rules limitations, so that the CKB contains RGBppLock cell and UTXO on BTC are anchored. The specific process is as follows:

1. The user generates the transaction content to be sent on CKB, and then calculates the commitment based on the transaction content.
2. The user uses the computed commitment to send a transaction UTXO with an OPRETURN to anchor the asset.
3. After the user sends the transaction on BTC and confirms it, the user generates a real ckb_tx with the generated tx_id and content and sends it to the CKB chain for anchoring. For BTC-Time-Lock, the purpose of this unlock script is to prevent transactions on BTC from being reorg, where the parameter after means that it can only be unlocked after several block confirmations. (after>=6)

4 Findings

RGB-1 RGBpplock Cell Binding to Commitment

Severity: Informational

Status: Acknowledged

Code Location:

crates/core/src/rgbpp.rs#8-10

Descriptions:

It is possible to have RGBpplock bind to unintended OP_RETURN(commitment) output that cannot be spent. And when bound this way, the rgbpplock's cell can't be unlocked.

Suggestion:

A check can be added to prevent rgpbb-lock from binding to an OP_RETURN output.

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.