



CBD Cash Protocol

Smart Contract Security Audit

April, 2021
[TechRate](#)

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by CBD Cash Protocol to perform an audit of smart contracts:

- <https://github.com/cbdcash/cbd-contracts/blob/1215e5f2906e3ee70e9023c2b154b711dd1cfb5d/contracts/Bond.sol>
- <https://github.com/cbdcash/cbd-contracts/blob/1215e5f2906e3ee70e9023c2b154b711dd1cfb5d/contracts/Dollar.sol>
- <https://github.com/cbdcash/cbd-contracts/blob/1215e5f2906e3ee70e9023c2b154b711dd1cfb5d/contracts/Boardroom.sol>
- <https://github.com/cbdcash/cbd-contracts/blob/1215e5f2906e3ee70e9023c2b154b711dd1cfb5d/contracts/OracleSinglePair.sol>
- <https://github.com/cbdcash/cbd-contracts/blob/1215e5f2906e3ee70e9023c2b154b711dd1cfb5d/contracts/Share.sol>
- <https://github.com/cbdcash/cbd-contracts/blob/1215e5f2906e3ee70e9023c2b154b711dd1cfb5d/contracts/ShareRewardPool.sol>
- <https://github.com/cbdcash/cbd-contracts/blob/1215e5f2906e3ee70e9023c2b154b711dd1cfb5d/contracts/Treasury.sol>

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Issues Checking Status

№	Issue description.	Checking status
1	Compiler warnings.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issues found.

Owner privileges

- ☐ Owner can [change](#) the operator in the Bond contract.
- ☐ Operator can [mint](#) any amount of bCBD tokens in the Bond contract.
- ☐ Owner can [change](#) the operator in the Dollar contract.
- ☐ Operator can [mint](#) any amount of cCBD tokens in the Dollar contract.
- ☐ Operator can [change](#) the withdrawal and reward lockup epochs.
- ☐ Operator can [withdraw](#) foreign tokens(except Dollar and Share) from the contract.
- ☐ Operator can [change](#) the epoch's period.
- ☐ Owner can [change](#) the operator in the Share contract.
- ☐ Operator can [distribute](#) farming pool reward allocation to any address.
- ☐ Dev in the Share contract can change the [community](#) and [dev](#) address.
- ☐ Operator can [withdraw](#) tokens from the ShareRewardPool contract. Also he can withdraw lp tokens when 6 months will pass after pool ends.
- ☐ Operator can [change](#) the operator address in the Treasury contract.
- ☐ Operator can [change](#) the Boardroom contract to the new not audited contract.
- ☐ Operator can [change](#) the dollar oracle contract to the new not audited contract.
- ☐ Operator can [change](#) the dollar price ceiling.
- ☐ Operator can [change](#) the max supply expansion percents.
- ☐ Operator can [change](#) the bond depletion floor percent.
- ☐ Operator can [change](#) the max supply contraction percent.
- ☐ Operator can [change](#) the max dept ratio percent.
- ☐ Operator can [change](#) the extra funds.
- ☐ Operator can [change](#) the allocate seigniorage salary.
- ☐ Operator can [change](#) the max discount rate.
- ☐ Operator can [change](#) the max premium rate.

- ❑ Operator can [change](#) the discount percent.
- ❑ Operator can [change](#) the premium rate.
- ❑ Operator can [migrate](#) to the new not audited contract all the funds and operator status over dollar, bond and share contracts.
- ❑ Operator can [withdraw](#) tokens (except dollar, bond, share) from the Treasury contract.

Recommendations

- ❑ [_setupDecimals](#) function in the Bond contract has no usages and could be removed, as decimals value will be set in constructor and not changed after.
- ❑ [_beforeTokenTransfer](#) function in the Bond contract is empty and not overridden, so its usages could be removed.
- ❑ [_setupDecimals](#) function in the Dollar contract has no usages and could be removed, as decimals value will be set in constructor and not changed after.
- ❑ [_beforeTokenTransfer](#) function in the Dollar contract is empty and not overridden, so its usages could be removed.
- ❑ Add operator [changed](#) event.
- ❑ [_setupDecimals](#) function in the Share contract has no usages and could be removed, as decimals value will be set in constructor and not changed after.
- ❑ [_beforeTokenTransfer](#) function in the Share contract is empty and not overridden, so its usages could be removed.

Conclusion

Smart contracts do not contain any high severity issues! Ownership transferred to the zero address.

Techrate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.