BTCD

Security Assessment

CertiK Assessed on Oct 28th, 2025

CertiK Assessed on Oct 28th, 2025

BTCD

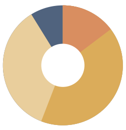
The security assessment was prepared by CertiK.

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Bitcoin | EVM Compatible	Manual Review, Static Analysis

LANGUAGE	TIMELINE
Solidity	Preliminary comments published on 10/08/2025 Final report published on 10/28/2025

Vulnerability Summary



34	25	0	9	0
Total Findings	Resolved	Partially Resolved	Acknowledged	Declined

2	Centralization	2 Acknowledged	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.
3	Major	3 Resolved	Major risks may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.
14	Medium	13 Resolved, 1 Acknowledged	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
12	Minor	8 Resolved, 4 Acknowledged	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.
3	Informational	1 Resolved, 2 Acknowledged	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 | BTCD

CODEBASE | BTCD

Repository

https://github.com/nbwfoundation/ArbitrationProtocol

https://github.com/nbwfoundation/btcd-stablecoins

https://github.com/nbwfoundation/loan_unlock_tx

Commit

2b13defab3cbd768ba31d6ce737c4adeef9ef2d4

ff7fd27c9f30c0e598a13d332163b0dcd6d9387f

69a35a298795f0801ab82091ea08f1d05c3d65a2

Audit Scope

The file in scope is listed in the appendix.

APPROACH & METHODS | BTCD

This audit was conducted for BTCD to evaluate the security and correctness of the smart contracts associated with the BTCD 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.

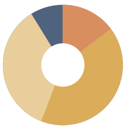
The review process emphasized the following areas:

- 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 | BTCD



34	0	2	3	14	12	3
Total Findings	Critical	Centralization	Major	Medium	Minor	Informational

This report has been prepared for BTCD to identify potential vulnerabilities and security issues within the reviewed codebase. During the course of the audit, a total of 34 issues were identified. Leveraging a combination of Manual Review & Static Analysis the following findings were uncovered:

ID	Title	Category	Severity	Status
BTC-01	**Centralized Control Of Contract Upgrade**	**Centralization**	**Centralization**	**Acknowledged**
BTC-77	**Centralization Related Risks**	**Centralization**	**Centralization**	**Acknowledged**
BTC-26	Unrestricted InterestReceiver Lets Anyone Redirect Protocol Fees In New Lend Orders	Logical Issue	Major	Resolved
BTC-51	Missing Restriction On RepaidExpireTime Relative To LockTime1 Could Put Borrower At Risk	Logical Issue	Major	Resolved
BTC-52	Unlimited Token Mint To Arbitrary Address Is Possible	Volatile Code, Financial Manipulation	Major	Resolved
BTC-06	Arbitrator-Controlled Revenue Address Can Permanently DoS Settlement And Trap Funds	Denial of Service	Medium	Resolved
BTC-07	Zero ArbitratorFee Causes Permanent Deposit Lock While Marking The Transaction Completed	Logical Issue	Medium	Resolved
BTC-12	Pre-Activation Slashing Enabled By Accepting ToBeActive Status With Empty UTXO Arrays	Logical Issue	Medium	Resolved

ID	Title	Category	Severity	Status
BTC-13	`registerArbitratorByStakeNFT()` Never Deposits NFTs, Enabling Registration Without Staking	Logical Issue	Medium	Resolved
BTC-24	Weak Script Matching	Design Issue	Medium	Resolved
BTC-27	Unbounded State Growth Via Public Decoder Enables Storage-Bloat DoS	Denial of Service	Medium	Resolved
BTC-28	Lack Of Public Key Validation	Logical Issue	Medium	Resolved
BTC-29	Borrow Allowed After Repay Window Expired Due To Wrong Base Timestamp In CalcStepsOverTime	Logical Issue	Medium	Resolved
BTC-30	Function Calls User-Provided Addresses With No Access Control Modifier	Access Control	Medium	Resolved
BTC-44	No Cap On Fees	Logical Issue	Medium	Resolved
BTC-53	Zero ArbiterFee Enables DOS On Orders	Denial of Service	Medium	Acknowledged
BTC-57	Missing Condition In If Statement	Logical Issue, Volatile Code	Medium	Resolved
BTC-58	Inconsistent And Weak Require Statements	Logical Issue, Inconsistency	Medium	Resolved
BTC-76	`rawData` Is Never Bound To The Verified Merkle Leaf In The Pledge And Unlock Proof Paths	Logical Issue	Medium	Resolved
BTC-18	Unlimited Contract Spawning By Repeatedly Calling CreateStakingContract Because New Contracts Start Inactive	Logical Issue	Minor	Resolved
BTC-25	Inconsistent P2WSH Redeem Script Construction	Inconsistency	Minor	Resolved

ID	Title	Category	Severity	Status
BTC-32	Lack Of Storage Gap Or NameSpaced Storage Layout In Upgradeable Contract	Design Issue	Minor	Acknowledged
BTC-33	`initialize()` Is Unprotected	Logical Issue	Minor	Resolved
BTC-38	Abstract Base Contract Should Not Use Modifier `initializer()`	Coding Issue	Minor	Resolved
BTC-59	The Surplus Native Tokens Are Not Returned	Design Issue	Minor	Resolved
BTC-60	Incorrect Role Management	Logical Issue	Minor	Acknowledged
BTC-62	Unreachable If Condition	Coding Issue	Minor	Acknowledged
BTC-63	Inconsistent Code And Comment	Inconsistency	Minor	Resolved
BTC-64	Limitations Of Collateral Comparison At A Point In Time	Design Issue	Minor	Acknowledged
BTC-65	Ineffective Require Statement	Logical Issue	Minor	Resolved
BTC-67	Lack Of Access Control In Event Emit With Arbitrary Parameter	Volatile Code	Minor	Resolved
BTC-23	Presence Of Debugging Code	Logical Issue	Informational	Resolved
BTC-69	Missing Emit Events	Coding Style	Informational	Acknowledged
BTC-71	Unused Modifier	Coding Issue	Informational	Acknowledged

APPENDIX | BTCD

Audit Scope

nbwfoundation/ArbitrationProtocol
contracts/core/ConfigManager.sol
contracts/core/ArbitratorManager.sol
contracts/core/CompensationManager.sol
contracts/core/TransactionManager.sol
contracts/core/ArbitratorWhitelist.sol
contracts/core/AssetManager.sol
contracts/core/DAppRegistry.sol
contracts/core/TokenWhitelist.sol
contracts/ArbitrationProtocol.sol
contracts/MultiSignWallet.sol
contracts/Timelock.sol

nbwfoundation/btcd-stablecoins
contracts/interest/Interest.sol
contracts/issuer/Issuer.sol
contracts/order/Order.sol
contracts/order/OrderProxy.sol
contracts/orderTools/LoanTools.sol
contracts/stableCoin/StableCoin.sol
contracts/Pledge.sol

nbwfoundation/btcd-stablecoins
contracts/order/OrderFactory.sol
contracts/orderTools/GetLoanTools.sol
contracts/proof/ProofSubmitters.sol
contracts/scriptBuilder/LoanScript.sol
contracts/staking/StakingFactory.sol
contracts/LoanContract.sol
contracts/issuer/IIssuer.sol
contracts/libraries/ConfigManagerKeys.sol
contracts/libraries/DataTypes.sol
contracts/libraries/Errors.sol
contracts/order/IOrder.sol
contracts/order/IOrderFactory.sol
contracts/scriptBuilder/ILoanScript.sol
contracts/stableCoin/IStableCoin.sol
contracts/staking/Staking.sol
contracts/utils/Bech32.sol
contracts/utils/Bytes.sol
contracts/utils/BytesLib.sol
contracts/utils/ContractConst.sol
contracts/utils/Memory.sol
contracts/utils/MerkleProof.sol
contracts/utils/MerkleVerifier.sol

nbwfoundation/btcd-stablecoins
contracts/utils/MyMath.sol
contracts/utils/TransferHelper.sol
contracts/MultiSignWallet.sol
contracts/Multicall3.sol
contracts/Timelock.sol

nbwfoundation/loan_unlock_tx
contracts/btcAddress/BtcAddress.sol
contracts/MsgTxSerialize.sol
contracts/btcAddress/ScriptBuilder.sol
contracts/btcScript/Opcode.sol
contracts/btcScript/SigHash.sol
contracts/btcTx/BtcConst.sol
contracts/btcTx/BtcTx_Factory.sol
contracts/btcTx/MsgTx.sol
contracts/LoanUnLock.sol

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.
Coding Issue	Coding Issue findings are about general code quality including, but not limited to, coding mistakes, compile errors, and performance issues.
Denial of Service	Denial of Service findings indicate that an attacker may prevent the program from operating correctly or responding to legitimate requests.

Categories	Description
Access Control	Access Control findings are about security vulnerabilities that make protected assets unsafe.
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.
Financial Manipulation	Financial Manipulation findings indicate issues in design that may lead to financial losses.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.

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.