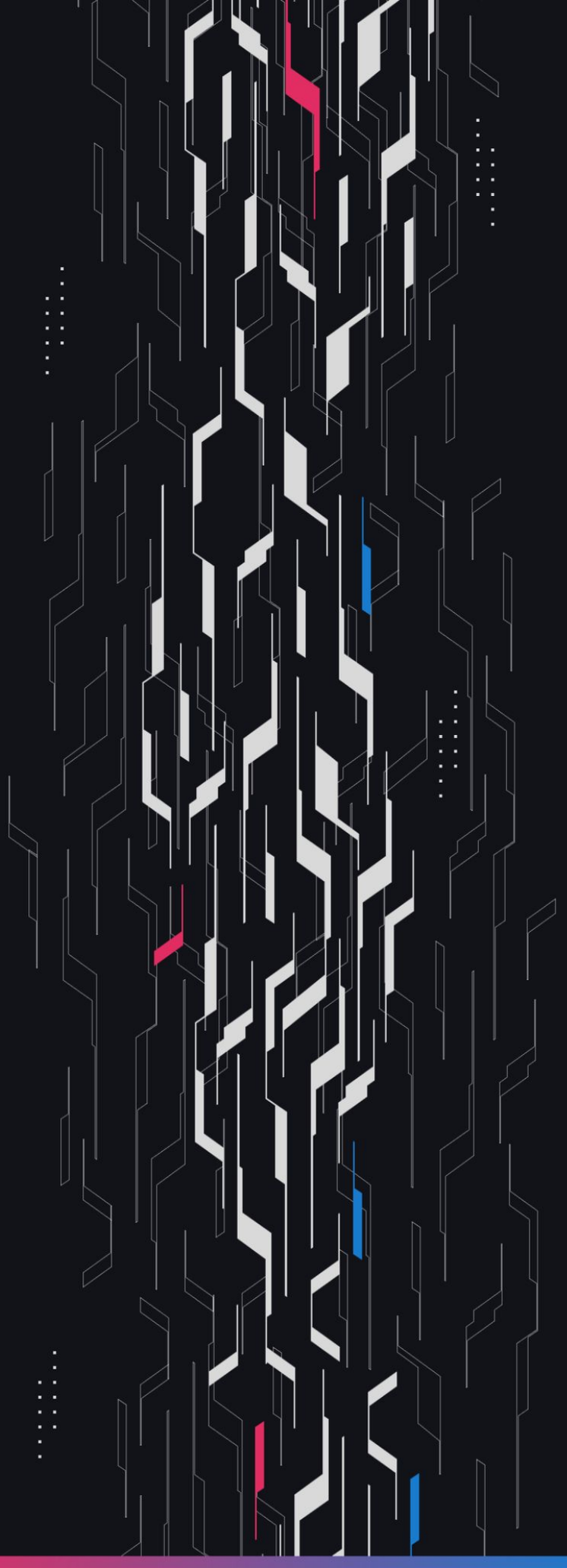
GA GUARDIAN

BTCX

Token Review

Security Assessment

December 25th, 2025



Summary

Audit Firm Guardian

Prepared By Owen Thurm

Client Firm BTCX

Final Report Date December 25, 2025

Audit Summary

BTCX engaged Guardian to review the security of their BTCX Token. From the 15th of December to the 18th of December, an auditor reviewed the source code in scope. All findings have been recorded in the following report.

Confidence Ranking

Given the lack of High and Critical issues detected during the main review, Guardian assigns a Confidence Ranking of 5 to the protocol. Guardian advises the protocol to consider periodic review with future changes. For detailed understanding of the Guardian Confidence Ranking, please see the rubric on the following page.

Note: Fixes to the findings uncovered in the remediation review have not been reviewed by Guardian. Guardian recommends the client either perform an amended follow-up review period to focus on the fixes to remediations findings or seek a follow-up audit from another team.

✅ Verify the authenticity of this report on Guardian's GitHub: https://github.com/guardianaudits

Guardian Confidence Ranking

Confidence Ranking	Definition and Recommendation	Risk Profile
5: Very High Confidence	Codebase is mature, clean, and secure. No High or Critical vulnerabilities were found. Follows modern best practices with high test coverage and thoughtful design. **Recommendation:** Code is highly secure at time of audit. Low risk of latent critical issues.	0 High/Critical findings and few Low/Medium severity findings.
4: High Confidence	Code is clean, well-structured, and adheres to best practices. Only 1 Significant issue was uncovered per week. Design patterns are sound, and test coverage is strong. **Recommendation:** Suitable for deployment after remediations; consider periodic review with changes.	0-1 High/Critical findings per engagement week and little to no Medium severity issues. Varied Low severity findings.
3: Moderate Confidence	Medium-severity and occasional High-severity issues found. Code is functional, but there are concerning areas (e.g., weak modularity, risky patterns). No critical design flaws, though some patterns could lead to issues in edge cases. **Recommendation:** Address issues thoroughly and consider a targeted follow-up audit depending on code changes.	1-2 High/Critical findings per engagement week.
2: Low Confidence	Code shows frequent emergence of Critical/High vulnerabilities. Audit revealed recurring anti-patterns, weak test coverage, or unclear logic. These characteristics suggest a high likelihood of latent issues. **Recommendation:** Post-audit development and a second audit cycle are strongly advised.	2-4 High/Critical findings per engagement week. Or additional High/Critical findings uncovered in remediation review which have not been resolved and confirmed by Guardian.
1: Very Low Confidence	Code has systemic issues. Multiple High/Critical findings (≥5/week), poor security posture, and design flaws that introduce compounding risks. Safety cannot be assured. **Recommendation:** Halt deployment and seek a comprehensive re-audit after substantial refactoring.	≥5 High/Critical findings and overall systemic flaws.

Table of Contents

Project Overview

Project Summary

Project Name	BTCX
Language	Solidity
Codebase	https://github.com/BTCX-Investment-Ltd/btcx-digital-currency
Commit(s)	Main Review commit: c259f65a4a2d095a987fbdc0e180daa3e012d868 Remediation Review commit: 3ff5966078d12ce873fb22314786ceb249a7578d

Audit Summary

Delivery Date	December 25, 2025
Audit Methodology	Static Analysis, Manual Review, Test Suite, Contract Fuzzing

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Low	0	0	0	0	0	0
Info	4	0	0	2	0	2

Audit Scope & Methodology

```
contract,source,total,comment
btcx-digital-currency/contracts/BTCXDigitalCurrency.sol,14,22,5
source count: {
  total: 22,
  source: 14,
  comment: 5,
  single: 15,
  block: 11,
  mixed: 0,
  empty: 18,
  todo: 0,
  blockEmpty: 0,
  commentToSourceRatio: 0.35714285714285715
}
```

Audit Scope & Methodology

Vulnerability Classifications

Severity	Impact: *High*	Impact: *Medium*	Impact: *Low*
Likelihood: *High*	🔴 Critical	🟠 High	🟡 Medium
Likelihood: *Medium*	🟠 High	🟡 Medium	🟢 Low
Likelihood: *Low*	🟡 Medium	🟢 Low	🟢 Low

Impact

High Significant loss of assets in the protocol, significant harm to a group of users, or a core functionality of the protocol is disrupted.

Medium A small amount of funds can be lost or ancillary functionality of the protocol is affected. The user or protocol may experience reduced or delayed receipt of intended funds.

Low Can lead to any unexpected behavior with some of the protocol's functionalities that is notable but does not meet the criteria for a higher severity.

Likelihood

High The attack is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount gained or the disruption to the protocol.

Medium An attack vector that is only possible in uncommon cases or requires a large amount of capital to exercise relative to the amount gained or the disruption to the protocol.

Low Unlikely to ever occur in production.

Audit Scope & Methodology

Methodology

Guardian is the ultimate standard for Smart Contract security. An engagement with Guardian entails the following:

- Two competing teams of Guardian security researchers performing an independent review.
- A dedicated fuzzing engineer to construct a comprehensive stateful fuzzing suite for the project.
- An engagement lead security researcher coordinating the 2 teams, performing their own analysis, relaying findings to the client, and orchestrating the testing/verification efforts.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts. Comprehensive written tests as a part of a code coverage testing suite.
- Contract fuzzing for increased attack resilience.

Findings & Resolutions

ID	Title	Category	Severity	Status
I-01	Unfixed Pragma	Best Practices	Info	Resolved
I-02	Readability Improvements	Best Practices	Info	Resolved
I-03	Unnecessary ERC20 Inheritance	Warning	Info	Acknowledged
I-04	Unnecessary Minting Event	Events	Info	Acknowledged

I-01 | Unfixed Pragma

Category	Severity	Location	Status
Best Practices	Info	BTCXDigitalCurrency.sol	Resolved

Description

In order to clearly identify the Solidity version with which the contracts will be compiled, pragma directives should be fixed and consistent across files within a project.

To avoid unexpected changes in bytecode across deployments the pragma version of the `BTCXDigitalCurrency` contract should be fixed instead of the current unfixed `^0.8.27` specification.

Recommendation

Fix the exact version of Solidity that will be used to deploy the BTCX token in the `BTCXDigitalCurrency` file.

Resolution

BTCX Team: Resolved.

I-02 | Readability Improvements

Category	Severity	Location	Status
Best Practices	Info	BTCXDigitalCurrency.sol	Resolved

Description

The initial supply for the `BTCXDigitalCurrency` contract is 1.2 Billion tokens and this is represented as `1200000000 * 10 ** decimals()`.

However this formatting may prove not optimally readable for verifiers or readers.

Recommendation

Consider using underscores to clearly display the supply as 1.2 Billion as follows:

`1_200_000_000 * 10 ** decimals()`

Resolution

BTCX Team: Resolved.

I-03 | Unnecessary ERC20 Inheritance

Category	Severity	Location	Status
Warning	● Info	BTCXDigitalCurrency.sol	Acknowledged

Description

The `BTCXDigitalCurrency` inherits from `ERC20` as well as `ERC20Burnable` and `ERC20Permit`.

However, the direct `is ERC20` inheritance is not strictly necessary since both the `ERC20Burnable` and `ERC20Permit` contracts inherit from `ERC20` themselves.

Recommendation

Consider removing the direct `is ERC20` inheritance as it is not strictly necessary, however there is no harm in keeping it.

Resolution

BTCX Team: Acknowledged.

I-04 | Unnecessary Minting Event

Category	Severity	Location	Status
Events	Info	BTCXDigitalCurrency.sol	Acknowledged

Description

The constructor emits an `InitialMint` event upon minting the 1.2 Billion initial supply of tokens.

However, this initial event emission is not necessary because the `_mint` function itself emits a `Transfer` event where the `from` address is `address(0)` to indicate that this is a mint.

As this is the only time a mint can occur with the BTCX token, this is sufficient to represent the initial mint.

Recommendation

Consider removing the `InitialMint` event as it is redundant with the event emitted by `_mint`.

Resolution

BTCX Team: Acknowledged.

Disclaimer

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 Guardian 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. Guardian’s position is that each company and individual are responsible for their own due diligence and continuous security. Guardian’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 Guardian 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.

Notice that smart contracts deployed on the blockchain are not resistant from internal/external exploit. Notice that active smart contract owner privileges constitute an elevated impact to any smart contract’s safety and security. Therefore, Guardian does not guarantee the explicit security of the audited smart contract, regardless of the verdict.

About Guardian

Founded in 2022 by DeFi experts, Guardian is a leading audit firm in the DeFi smart contract space. With every audit report, Guardian upholds best-in-class security while achieving our mission to relentlessly secure DeFi.

To learn more, visit https://guardianaudits.com

To view our audit portfolio, visit https://github.com/guardianaudits

To book an audit, message https://t.me/guardianaudits