Avalon X

Security Assessment

CertiK Assessed on Aug 21st, 2025

CertiK Assessed on Aug 21st, 2025

Avalon X

The security assessment was prepared by CertiK.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Base	Ethereum (ETH)	Manual Review, Static Analysis

LANGUAGE	TIMELINE
Solidity	Preliminary comments published on 08/21/2025 Final report published on 08/21/2025

Vulnerability Summary

4	0	1	0	3	0
Total Findings	Resolved	Multi-Sig	Partially Resolved	Acknowledged	Declined

🟧	1	Centralization	1 Multi-Sig	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.
🟧	0	Major		Major risks may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.
🟨	0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
🟨	1	Minor	1 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.
🟦	2	Informational	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 | AVALON X

Summary

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

Findings

ECE-06 : Initial Token Distribution

ECE-07 : Missing Zero Address Validation

ECE-08 : Dead Code

ECE-09 : Inconsistent Naming Convention For Public Variable `_creator`

Optimizations

ECE-01 : State Variable Should Be Declared Constant

ECE-02 : State variables that could be declared immutable

ECE-03 : Unused Inheritance from Ownable Contract

ECE-04 : Unused State Variable `mintedByDxsale`

ECE-05 : Redundant `mintingFinishedPermanent` Flag and Ineffective Minting Guard

Appendix

Disclaimer

CODEBASE | AVALON X

Repository

eth_base

Commit

0xbbb5dc0584e825b11a15c386208f7370203a1486

AUDIT SCOPE | AVALON X

mainnet
DxStandardToken.sol

APPROACH & METHODS | AVALON X

This report has been prepared for Avalon X to discover issues and vulnerabilities in the source code of the Avalon X project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Manual Review and Static Analysis techniques.

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.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Testing the smart contracts against both common and uncommon attack vectors;
- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

FINDINGS | AVALON X

Total Findings	Critical	Centralization	Major	Medium	Minor	Informational
4	0	1	0	0	1	2

This report has been prepared for Avalon X to identify potential vulnerabilities and security issues within the reviewed codebase. During the course of the audit, a total of 4 issues were identified. Leveraging a combination of Manual Review & Static Analysis the following findings were uncovered:

ID	Title	Category	Severity	Status
ECE-06	**Initial Token Distribution**	**Centralization**	**Centralization**	● **3/3 Multi-Sig**
ECE-07	Missing Zero Address Validation	Volatile Code	Minor	● Acknowledged
ECE-08	Dead Code	Coding Issue	Informational	● Acknowledged
ECE-09	Inconsistent Naming Convention For Public Variable `_creator`	Coding Style	Informational	● Acknowledged

ECE-06 | Initial Token Distribution

Category	Severity	Location	Status
Centralization	● **Centralization**	**DxStandardToken.sol: 478**	● **3/3 Multi-Sig**

Description

All `DxStandardToken` tokens are initially sent to a single externally owned account (EOA), introducing a centralization risk. The owner of this EOA can unilaterally distribute tokens without community consensus, and if the account is ever compromised, an attacker could steal and sell the tokens, potentially causing significant harm to the project and its stakeholders.

Recommendation

It is recommended that the team be transparent regarding the initial token distribution process. The token distribution plan should be published in a public location that the community can access. The team should make efforts to restrict access to the private keys of the deployer account or EOAs. A multi-signature (⅔, ⅗) wallet can be used to prevent a single point of failure due to a private key compromise. Additionally, the team can lock up a portion of tokens, release them with a vesting schedule for long-term success, and deanonymize the project team with a third-party KYC provider to create greater accountability.

Alleviation

[Certik, 08/21/2025]: The token `DxStandardToken` deployed at 0xbbb5dc0584e825b11a15c386208f7370203a1486.

Total Supply: 2,000,000,000 tokens

Owner Address: 0x5E2C57fa32a6583bD4FC51dF49465b60cccfF776

The multiwallet uses a 3 out of 3 multisignature scheme for transaction approvals. Signers:

- 0x9806b347Fa880476364EFBc973fA997235EC68d9
- 0x4da821719469c83376867471aa64A95b8439A80e
- 0x2A7DfFCD146883A9Cb7079881C0a7252D79D3DbD

ECE-07 | Missing Zero Address Validation

Category	Severity	Location	Status
Volatile Code	● Minor	DxStandardToken.sol: 476	● Acknowledged

Description

The cited address input is missing a check that it is not `address(0)` .

Recommendation

We recommend adding a check the passed-in address is not `address(0)` to prevent unexpected errors.

Alleviation

[Avalon X, 08/12/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

ECE-08 | Dead Code

Category	Severity	Location	Status
Coding Issue	● Informational	DxStandardToken.sol: 681~692	● Acknowledged

Description

One or more internal functions are not used.

```
681     function _burn(address account, uint256 amount) internal virtual {
```

Recommendation

We recommend removing those unused functions.

Alleviation

[Avalon X, 08/12/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

ECE-09 | Inconsistent Naming Convention For Public Variable `_creator`

Category	Severity	Location	Status
Coding Style	● Informational	DxStandardToken.sol: 464	● Acknowledged

Description

The variable `_creator` is marked as public but uses a leading underscore, which contradicts common naming conventions where underscores typically denote private or internal variables. This inconsistency can confuse developers and auditors about the variable's intended visibility and purpose, reducing code readability and increasing the risk of misinterpretation during integration or review.

Recommendation

We recommend renaming `_creator` to `creator` to align with standard naming conventions for public variables and improve code clarity.

Alleviation

[Avalon X, 08/12/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

OPTIMIZATIONS | AVALON X

ID	Title	Category	Severity	Status
ECE-01	State Variable Should Be Declared Constant	Coding Issue	Optimization	● Acknowledged
ECE-02	State Variables That Could Be Declared Immutable	Coding Issue	Optimization	● Acknowledged
ECE-03	Unused Inheritance From Ownable Contract	Code Optimization	Optimization	● Acknowledged
ECE-04	Unused State Variable `mintedByDxsale`	Gas Optimization	Optimization	● Acknowledged
ECE-05	Redundant `mintingFinishedPermanent` Flag And Ineffective Minting Guard	Gas Optimization	Optimization	● Acknowledged

ECE-01 | State Variable Should Be Declared Constant

Category	Severity	Location	Status
Coding Issue	● Optimization	DxStandardToken.sol: 458	● Acknowledged

Description

State variables that never change should be declared as `constant` to save gas.

```
458        bool public mintedByDxsale = true;
```

- `mintedByDxsale` should be declared `constant`.

Recommendation

We recommend adding the `constant` attribute to state variables that never change.

Alleviation

[Avalon X, 08/12/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

ECE-02 | State Variables That Could Be Declared Immutable

Category	Severity	Location	Status
Coding Issue	● Optimization	DxStandardToken.sol: 460, 463, 464	● Acknowledged

Description

State variables that are not updated following deployment should be declared immutable to save gas.

Recommendation

Add the immutable attribute to state variables that never change or are set only in the constructor.

Alleviation

[Avalon X, 08/12/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

ECE-03 Unused Inheritance From Ownable Contract

Category	Severity	Location	Status
Code Optimization	● Optimization	DxStandardToken.sol: 453	● Acknowledged

Description

`Ownable` is inherited but not utilized in the contract, introducing unnecessary bytecode and potentially misleading future auditors or developers into thinking ownership based access control is implemented. This unused inheritance can lead to confusion and bloated contracts, and should be removed if ownership logic is not intended.

Recommendation

We recommend removing the unused Ownable inheritance to reduce contract size and avoid misleading assumptions about access control mechanisms.

Alleviation

[Avalon X, 08/12/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

ECE-04 | Unused State Variable `mintedByDxsale`

Category	Severity	Location	Status
Gas Optimization	● Optimization	DxStandardToken.sol: 458	● Acknowledged

Description

`mintedByDxsale` is declared as a public state variable and initialized to `true`, but it is never modified or used elsewhere in the contract, indicating it serves no functional purpose. Leaving unused state variables in the contract can increase gas costs during deployment and may confuse readers or auditors about their intended role.

Recommendation

We recommend removing the unused `mintedByDxsale` variable to optimize contract size and improve code clarity.

Alleviation

[Avalon X, 08/12/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

ECE-05 | Redundant `mintingFinishedPermanent` Flag And Ineffective Minting Guard

Category	Severity	Location	Status
Gas Optimization	● Optimization	DxStandardToken.sol: 460, 479, 660	● Acknowledged

Description

`mintingFinishedPermanent` is set to `true` during the constructor and never changed afterward, while the `_mint()` function that references it is marked `internal` and not exposed externally. This makes the require check guarding `_mint()` ineffective in practice and the `mintingFinishedPermanent` flag redundant, adding unnecessary complexity and deployment cost without contributing to security or functionality.

Recommendation

We recommend removing the `mintingFinishedPermanent` flag and its associated require check to reduce contract complexity and eliminate unnecessary code.

Alleviation

[Avalon X, 08/12/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

APPENDIX | AVALON X

Finding Categories

Categories	Description
Gas Optimization	Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.
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.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases and may result in vulnerabilities.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.

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.