

Digital Asset Registry Daml Audit

Security Assessment

CertiK Assessed on Aug 13th, 2026





Certik Assessed on Aug 13th, 2026

Digital Asset Registry Daml Audit

The security assessment was prepared by Certik.

Executive Summary

TYPES

Utility

ECOSYSTEM

Canton

METHODS

Manual Review, Static Analysis

LANGUAGE

Daml

TIMELINE

Preliminary comments published on 07/02/2026

Final report published on 08/21/2026

Vulnerability Summary



8

Total Findings

3

Resolved

0

Partially Resolved

5

Acknowledged

0

Declined

0 Centralization

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.

4 Minor

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.

4 Informational

3 Resolved, 1 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.

CODEBASE | DIGITAL ASSET REGISTRY DAML AUDIT

Repository

<https://github.com/DACH-NY/canton-network-apps/tree/v0.12.15/app>

Commit

[503c4f32a38a4bfec23698684a1b5ff565c80e2b](#)

Audit Scope

The files in scope are listed in the appendix.

APPROACH & METHODS | DIGITAL ASSET REGISTRY DAML AUDIT

This audit was conducted for Digital Asset to evaluate the security and correctness of the smart contracts associated with the Digital Asset Registry Daml Audit 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.

APPENDIX | DIGITAL ASSET REGISTRY DAML AUDIT

Audit Scope

DACH-NY/canton-network-apps

- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Rule/Transfer.daml
- registry/utility-registry-holding-v0/src/main/daml/Utility/Registry/Holding/V0/Holding.daml
- registry/utility-registry-holding-v0/src/main/daml/Utility/Registry/Holding/V0/Util.daml
- registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Model/Burn.daml
- registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Model/Mint.daml
- registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Model/Transfer.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Configuration/Instrument.daml
- registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Service/Provider.daml
- registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Service/Registrar.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Configuration/AppReward.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Holding/Allocation.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Holding/Burn.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Holding/ForceTransfer.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Holding/Lock.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Holding/Mint.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Holding/TokenApiUtils.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Holding/Transfer.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Holding/Unlock.daml
- registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Types.daml

DACH-NY/canton-network-apps

	registry/utility-registry-v0/src/main/daml/Utility/Registry/V0/Util.daml
	registry/utility-registry-holding-v0/src/main/daml/Utility/Registry/Holding/V0/TokenApiUtils.daml
	registry/utility-registry-holding-v0/src/main/daml/Utility/Registry/Holding/V0/Types.daml
	registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Configuration/Operator.daml
	registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Configuration/Provider.daml
	registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Configuration/Registrar.daml
	registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Model/TransferPreapproval.daml
	registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Service/AllocationFactory.daml
	registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Service/Enforcement.daml
	registry/utility-registry-app-v0/src/main/daml/Utility/Registry/App/V0/Service/Holder.daml

Finding Categories

Categories	Description
Inconsistency	Inconsistency findings refer to different parts of code that are not consistent or code that does not behave according to its specification.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.
	No description available.
Code Optimization	No description available.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases and may result in vulnerabilities.

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.

Elevate Your Web3 Journey

CertiK is the largest Web3 security platform combining formal verification with audits and comprehensive security solutions.

Digital Asset Registry Daml Audit Security Assessment | CertiK Assessed on Aug 13th, 2026 | Copyright © CertiK

