Minswap - withdraw0 feature

Preliminary Comments

Draft (Internal Use Only)

CertiK Assessed on Aug 29th, 2025

CertiK Assessed on Aug 29th, 2025

Minswap - withdraw0 feature

These preliminary comments were prepared by CertiK.

Executive Summary

TYPES	ECOSYSTEM	METHODS
DEX	Cardano (ADA)	Manual Review

LANGUAGE	TIMELINE
Aiken	Preliminary comments published on 02/27/2025

Vulnerability Summary

6	0	0	6	0	0
Total Findings	Resolved	Partially Resolved	Acknowledged	Declined	Pending

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.
1	Major	1 Acknowledged	Major risks may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.
3	Medium	3 Acknowledged	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.
1	Informational	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.
0	Discussion		The impact of the issue is yet to be determined, hence requires further clarifications from the project team.

TABLE OF CONTENTS | MINSWAP - WITHDRAW0 FEATURE

CODEBASE | MINSWAP - WITHDRAW0 FEATURE

Repository

(https://github.com/scisamir/minswap-dex-v2/tree/11b18d887dc97ec39afdf70e5614a8771c1d8f5a)

Commit

11b18d887dc97ec39afdf70e5614a8771c1d8f5a

AUDIT SCOPE | MINSWAP - WITHDRAW0 FEATURE

scisamir/minswap-dex-v2
validators/authen_minting_policy.ak
validators/pool_validator.ak
validators/always_success.ak
validators/factory_validator.ak
validators/order_validator.ak
validators/sample_multi_sign.ak

APPROACH & METHODS | MINSWAP - WITHDRAW0 FEATURE

This report has been prepared for Minswap to discover issues and vulnerabilities in the source code of the Minswap - withdraw0 feature 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 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 | MINSWAP - WITHDRAW0 FEATURE

6	0	0	1	3	1	1	0
Total Findings	Critical	Centralization	Major	Medium	Minor	Informational	Discussion

This report has been prepared for Minswap to identify potential vulnerabilities and security issues within the reviewed codebase. During the course of the audit, a total of 6 issues were identified. Leveraging a combination of Manual Review the following findings were uncovered:

ID	Title	Category	Severity	Status
VAL-02	**Centralization Related Risks**	**Centralization**	**Major**	**Acknowledged**
GLOBAL-01	Lack Of Documentation And Detailed Specifications Related To This Update	Coding Issue	Medium	Acknowledged
GLOBAL-02	Incomplete And Outdated Offchain Code	Coding Issue	Medium	Acknowledged
MWF-01	Potential Reserve And Order Inconsistency Due To CIP-113 Token Behaviors	Design Issue, Inconsistency	Medium	Acknowledged
MWF-02	CIP-113 Tokens Support Within A Single DEX Pool	Design Issue	Minor	Acknowledged
TYP-01	Potential For Multiple Roles Per Address	Access Control	Informational	Acknowledged

VAL-02 | Centralization Related Risks

Category	Severity	Location	Status
Centralization	Major	validators/authen_minting_policy.ak: 170~171; validators/pool_validator.ak: 36~37, 67~68, 180~181	Acknowledged

Description

Admin

In the validator `authen_minting_policy.spend()`, the role `admin` has the authority to spend the `GlobalSetting` token of the protocol, and therefore to update the Global Setting. In particular the `admin` can:

- change the list of authorized `batchers` as long as the list is not empty;
- change the address allowed to update the Pool's base fee and fee-sharing;
- change the address allowed to withdraw the Pool's fee-sharing;
- change the address allowed to update the Pool's credential;
- change the address allowed to update the Pool's dynamic fee;
- transfer the `admin` role to another address;

Any compromise to the `admin` account may allow a hacker to take advantage of this authority and:

- transfer `admin` privileges to an address they control;
- grant the below privileges to addresses they control;

Batcher

In the validator `pool_validator.pool_batching_validator.withdraw()`, the role `batcher` has the authority to apply orders and validate the new state of the pool by:

- `Batching` to submit a batch of orders in a transaction;
- `MultiRouting` to trigger a multi swap order;

Any compromise to a `batcher` account may allow a hacker to take advantage of this authority and submit transactions, potentially allowing manipulation of the order of transactions.

Fee Updater

In the validator `pool_validator.validate_pool()` the `pool_fee_updater` can use the action:

- `UpdatePoolFee` to modify the pool fees;

Any compromise to the `pool_fee_updater` account may allow a hacker to take advantage of this authority and update a liquidity pool's fee.

Fee Taker

In the validator `pool_validator.withdraw()` the `fee_sharing_taker` can use the action:

- `WithdrawFeeSharing` to withdraw protocol fees and send them to any address;

Any compromise to the `fee_sharing_taker` account may allow a hacker to take advantage of this authority and steal the protocol fees.

Stake Key Updater

In the validator `pool_validator.validate_pool.withdraw()` the `pool_stake_key_updater` can use the action:

- `UpdatePoolStakeCredential` to change the stake credential of a pool;

Any compromise to the `pool_stake_key_updater` account may allow a hacker to use this authority and change the credentials of a pool.

Dynamic Fee Updater

In the validator `pool_validator.validate_pool.withdraw()` the `pool_dynamic_fee_updater` can use the action:

- `UpdateDynamicFee` to enable or disable the dynamic fees;

Any compromise to the `pool_dynamic_fee_updater` account may allow a hacker to use this authority and disallow `Batcher` to choose the fee's volatility in a batch transaction.

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged roles especially the `admin` to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via decentralized mechanisms.

The team should ensure total transparency about the `batcher` and `admin` roles, their mechanisms, and the potential risk through articles or blog posts.

They should set clear expectations for how the batcher is supposed to behave (e.g. ruling out front-running) and clarify how it can be monitored to mitigate unexpected events.

Alleviation

[Minswap, 08/08/2025]: Issue acknowledged. I won't make any changes for the current version.

GLOBAL-01 Lack Of Documentation And Detailed Specifications Related To This Update

Category	Severity	Location	Status
Coding Issue	Medium		Acknowledged

Description

High-level documentation is very important to understand the contract architecture, the interaction of on-chain and off-chain components, the economic model, etc. Detailed technical design documentation can help verify that the code implementation meets the specifications. Specifications include but are not limited to use cases, user stories, function interfaces, variable definitions, constant variable intervals, etc.

The codebase lacks sufficient documentation with the changes regarding the current implementation. Comprehensive documentation is essential for maintaining, auditing, and understanding the code. The absence of detailed specifications impedes our ability to fully assess the system's design and behavior.

Recommendation

Consider creating extensive documentation and adding comments that explain the variables, functions, and logic behind the calculation and implementation. We also recommend documenting the various program use cases with unit and integration tests. Documentation and test files can make some findings or discussions easier to understand.

Alleviation

[Minswap, 08/08/2025]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

GLOBAL-02 | Incomplete And Outdated Offchain Code

Category	Severity	Location	Status
Coding Issue	Medium		Acknowledged

Description

Using unit tests to test smart contracts is one of the best ways to identify potential logic errors and security vulnerabilities in the smart contract. The unit test files in folder `./tests` seem to be incomplete and the files in the folder `./src` are out of date.

Recommendation

We recommend the team to add more test cases to cover more test coverage and finish the incomplete tests.

Alleviation

[Minswap, 08/08/2025]: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement.

MWF-01 | Potential Reserve And Order Inconsistency Due To CIP-113 Token Behaviors

Category	Severity	Location	Status
Design Issue, Inconsistency	Medium		Acknowledged

Description

The current design supports tokens governed by CIP-113, which introduces programmable control over token behaviors such as freeze, seize, and thaw. While this allows more flexible asset control, it introduces risk when these tokens are stored within critical on-chain structures such as pool UTxOs and order UTxOs.

In the current design, each pool UTxO stores critical state variables inside its datum, such as: `total_liquidity` , and `reserve_a` , `reserve_b` .

These values are assumed to represent the balance of liquidity providers. However, when a CIP-113 token inside the pool becomes frozen or seized, the asset technically remains in the UTxO, but can no longer be used. The datum, however, may not reflect this reduction in effective reserves. This leads to divergence between the recorded pool state and the effective token reserves, which can lead to incorrect swap calculations, liquidity misreporting, or economic imbalance.

A similar issue applies to order UTxOs. If a CIP-113 token used in an order becomes frozen or seized, the order remains on-chain and may appear valid, but cannot be fulfilled, resulting in execution failure or inconsistency.

Recommendation

As CIP-113 has not yet been finalized, it is unclear whether behaviors like freeze, seize, and thaw will be validator-enforced logic, or upgradable policy-driven configurations. We recommend that the team provide additional documentation outlining how CIP-113 token states will be handled in the context of pool and order logic. We also encourage the team to closely track changes to CIP-113 and assess the implications on both datum consistency and reserve validity.

Alleviation

[Minswap, 08/08/2025]: The freeze, seize action works only if the authority is actually blocking the dex, if it's blocking a user the pool will be still available for trading since it's not frozen

MWF-02 | CIP-113 Tokens Support Within A Single DEX Pool

Category	Severity	Location	Status
Design Issue	Minor		Acknowledged

Description

The protocol may consider supporting multiple CIP-113 tokens within a single liquidity pool. While this could offer expanded trading options, managing multiple governed assets introduces significant design complexity.、

Managing multiple such tokens in parallel—especially under a shared validator or pool context could present challenges in consistency, validator coordination, and reserve integrity. The feasibility and safety of this type of pool design remain uncertain until the standard is more clearly defined.

Recommendation

We encourage the team to provide additional documentation outlining how support for multiple cip-113 tokens is expected to function. Clarifying assumptions around pool structure, validator responsibilities, and governance enforcement will help ensure predictable and secure behavior.

Alleviation

[Minswap, 08/08/2025]: The protocol will allow only ADA/CIP113 token or at most CIP113/CIP113 token.

TYP-01 | Potential For Multiple Roles Per Address

Category	Severity	Location	Status
Access Control	Informational	lib/amm_dex_v2/types.ak: 327~341	Acknowledged

Description

`GlobalSetting` type is intended to maintain a record of address permissions for specific sensitive actions. However, when setting or updating those addresses, there are no constraints to prevent a single address from being assigned multiple or even all roles. This concentration of privileges can lead to a higher degree of centralization and increases security risks if the address is compromised.

Recommendation

We recommend adding constraints to prevent an address from being set multiple times in `GlobalSetting`.

Alleviation

[Minswap, 08/08/2025]: Issue acknowledged. I won't make any changes for the current version.

APPENDIX | MINSWAP - WITHDRAW0 FEATURE

Finding Categories

Categories	Description
Coding Issue	Coding Issue findings are about general code quality including, but not limited to, coding mistakes, compile errors, and performance issues.
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.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.
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.