CERTIK

Security Assessment

Minswap Labs - dex v2

CertiK Assessed on May 2nd, 2024

CertiK Assessed on May 2nd, 2024

Minswap Labs - dex v2

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Exchange	Cardano (ADA)	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Aiken	Delivered on 05/02/2024	N/A

CODEBASE

https://github.com/minswap/minswap-dex-v2/

View All in Codebase Page

COMMITS

7cc7012bcf03a3baba8fc2320a5a7609352e2643

2fa7b1653a9d6dd9e0b9a3500f88529b2f6e511a

View All in Codebase Page

Vulnerability Summary

3 Total Findings	1 Resolved	0 Mitigated	0 Partially Resolved	2 Acknowledged	0 Declined

■ 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 can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
■ 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 Resolved	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.

TABLE OF CONTENTS | MINSWAP LABS - DEX V2

CODEBASE | MINSWAP LABS - DEX V2

▌ Repository

https://github.com/minswap/minswap-dex-v2/

▌ Commit

7cc7012bcf03a3baba8fc2320a5a7609352e2643

2fa7b1653a9d6dd9e0b9a3500f88529b2f6e511a

AUDIT SCOPE | MINSWAP LABS - DEX V2

9 files audited ● 3 files with Acknowledged findings ● 1 file with Resolved findings ● 5 files without findings

ID	Repo	File	SHA256 Checksum
● TYP	CertiKProject/certik-audit-projects	projects/minswap/lib/amm_dex_v2/types.ak	5c26c8d29893a48092fd72626e859efdf197 16ef93116209f4aa388c8caf90f0
● AUT	CertiKProject/certik-audit-projects	projects/minswap/validators/authen_minting_policy.ak	31927b82f4b2baff5f5b466b9e2a02a8666c 02543f90715d2cefb002bfae2add
● POL	CertiKProject/certik-audit-projects	projects/minswap/validators/pool_validator.ak	a2c5de9df342e3a6fc8aea0f46f237bd19180 f0cf5effa1ab5d69545fb36fe1f
● ORD	CertiKProject/certik-audit-projects	projects/minswap/lib/amm_dex_v2/order_validation.ak	990b7c564da0e51dae05cbed1d9900087f5 75d9b82d08db87ec7b9a734f15ce7
● MAT	CertiKProject/certik-audit-projects	projects/minswap/lib/amm_dex_v2/math.ak	319f75eabc0a9c77acea5f01b128de09612c d22c35cf1bbe690da5b1bc673249
● POO	CertiKProject/certik-audit-projects	projects/minswap/lib/amm_dex_v2/pool_validation.ak	688b316b0b91c3c2dab2cd37a0e4875718c 86a4e25cb5f861dfcc3b65d7d29f0
● UTI	CertiKProject/certik-audit-projects	projects/minswap/lib/amm_dex_v2/utils.ak	7c3aeb917c681aceb6a78eccc149d86cacc c68b0653af9db4682809b55649610
● FAC	CertiKProject/certik-audit-projects	projects/minswap/validators/factory_validator.ak	6c133d131463330abeb077bef8cb9a5deb9 0036a644f54ce85a0041c1a7a7d74
● ORE	CertiKProject/certik-audit-projects	projects/minswap/validators/order_validator.ak	6b37f7bac8f3b5bb153e2f25b86c03c81477 8020075505f3b74cb36024e8751f

APPROACH & METHODS | MINSWAP LABS - DEX V2

This report has been prepared for Minswap Labs to discover issues and vulnerabilities in the source code of the Minswap Labs - dex v2 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.

REVIEW NOTES | MINSWAP LABS - DEX V2

The audit was specifically targeted to assess the differences between the current and previous versions as specified by the client. Our examination focused exclusively on the changes made since the last audit. It is important to note that the security evaluation of the features and configurations approved in the previous audit were not included in the scope of this current assessment. This approach ensures that each modification is thoroughly evaluated for security implications and adherence to the best practices in blockchain security.

FINDINGS | MINSWAP LABS - DEX V2

	3	0	1	0	1	1
	Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Minswap Labs - dex v2. Through this audit, we have uncovered 3 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
MIN-01	**Centralization Related Risks**	**Centralization**	**Major**	● **Acknowledged**
ORD-01	Missing Check For Batcher Fee In Donation Orders	Design Issue	Minor	● Resolved
TYP-01	Potential For Multiple Roles Per Address	Access Control	Informational	● Acknowledged

MIN-01 │ CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	🟠 **Major**	**projects/minswap/lib/amm_dex_v2/types.ak: 298~312; projects/minswap/validators/authen_minting_policy.ak: 218~219; projects/minswap/validators/pool_validator.ak: 63~64, 64~65, 65~66, 114~115, 187~188**	⚪ **Acknowledged**

▌ Description

Admin

In the validator `authen_minting_policy.validate_spend_global_setting()` , 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.validate_pool_batching()` , 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.validate_pool()` 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()` 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()` 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 Team, 2024/04/27]: We plan to further decentralize the addresses in the Global Setting in the future. These addresses may include the Smart Contract introduced in the `authorize_license_holder` function.

The addresses in the Global Setting can be categorized as one of the following:

- **Public key address**: The updating transaction must be signed with the corresponding private key;
- **Validator script**: In this case, a UTxO must be spent from the address (the validation of the script must approve the spending);
- **Staking script**: The transaction is also accepted if any staking operation is approved by the script.

The Admin role is the highest role in the DEX contract, and Minswap Labs must use a Multi-Signature address for this role from Day 1, providing proof to the community to prevent a single person from controlling the DEX.

ORD-01 | MISSING CHECK FOR BATCHER FEE IN DONATION ORDERS

Category	Severity	Location	Status
Design Issue	● Minor	projects/minswap/lib/amm_dex_v2/order_validation.ak: 967~972	● Resolved

▌ Description

The function `validate_donation` only verifies the batcher fee for orders involving ADA in the asset pair (`asset_a`). The function deducts the batcher fee directly from `amount_a` when `asset_a` is ADA.

However, the function does not perform checks on `order_in_value` and `order_out_value` , leading to uncertainty about whether the batcher fee is correctly paid in all scenarios. This could potentially allow donation orders to bypass the batcher fee payment when ADA is not part of the asset pair, raising concerns about the intended behavior and fee enforcement within the contract.

▌ Recommendation

We recommended the team to clarify the intended behavior regarding the batcher fee for donation orders. If the batcher fee is mandatory for all donation orders, the `validate_donation` function should be updated to include checks on `order_in_value` and `order_out_value` to ensure that the fee is properly paid regardless of the asset pair involved.

▌ Alleviation

[CertiK, 2024/04/27]: The team heeded the advice and resolved the finding in commit 2fa7b1653a9d6dd9e0b9a3500f88529b2f6e511a.

TYP-01 | POTENTIAL FOR MULTIPLE ROLES PER ADDRESS

Category	Severity	Location	Status
Access Control	● Informational	projects/minswap/lib/amm_dex_v2/types.ak: 298~312	● 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 Team, 2024/04/27]: We plan to further decentralize the addresses in the Global Setting in the future. These addresses may include the Smart Contract introduced in the `authorize_license_holder` function.

In the future, a single Smart Contract might be responsible for multiple roles, so we have decided not to enforce the uniqueness of these roles.

OPTIMIZATIONS | MINSWAP LABS - DEX V2

ID	Title	Category	Severity	Status
ORD-02	Unoptimized Check	Code Optimization	Optimization	● Resolved

ORD-02 | UNOPTIMIZED CHECK

Category	Severity	Location	Status
Code Optimization	● Optimization	projects/minswap/lib/amm_dex_v2/order_validation.ak: 47~ 48	● Resolved

▌ Description

In `order_validation.get_optimized_swap_output_value()` , the following condition check:

```
47    if asset_a_policy_id == #"" && asset_a_asset_name == #"" {
```

uses empty strings to verify if `asset_a` is ADA, however the function `utils.is_ada_asset()` does the same verification.

▌ Recommendation

We recommend using directly `utils.is_ada_asset()` , `ada_policy_id` , and `ada_asset_name` .

▌ Alleviation

[CertiK, 2024/04/27]: The team heeded the advice and resolved the finding in commit 2fa7b1653a9d6dd9e0b9a3500f88529b2f6e511a.

APPENDIX | MINSWAP LABS - DEX V2

Finding Categories

Categories	Description
Access Control	Access Control findings are about security vulnerabilities that make protected assets unsafe.
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.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

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.

CertiK | **Securing** the **Web3** World

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading 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.