Batcher DEX

Marigold

Independent security assessment report

inference

Report version: 1.0 / date: 02.05.2023

inference

Table of contents

Version / Date	Description
1.0 / 02.05.2023	Final version.

Summary

Inference AG was engaged by Marigold to perform an independent security assessment of their Batcher DEX smart contact.

Inference AG performed the security assessment based on the agreed scope, following our approach and activities as outlined in the “Project overview” chapter between 14th March 2023 and 21th April 2023. Feedback from Marigold was received during the course of the assessment and Inference performed a follow-up assessment.

Based on our scope and our performed activities, our security assessment revealed a few observations, which, if resolved appropriately, may improve the quality of Marigold’s Batcher DEX smart contract.

This report only shows remaining open or partly resolved security issues and observations.

Overview on issues and observations

Details for each reported issue or observation can be obtained from the "Security issues" and "Observations" sections.

Row header	Severity / Status
Security issues	
There are no open known security issues.	
Observations	
O-MBA-001: Use of appropriate tokens	- / partially closed

Project overview

Scope

The scope of the security assessment was Marigold's Batcher DEX smart contract:

- Batcher DEX:
  batcher/batcher.mligo including all code and files in order to build the Batcher DEX smart contract with entrypoint "main"

Our initial assessment considered commit "007f3b401322b3824816e7a82e6997a61dd93a06" in the Batcher DEX source code repository https://github.com/marigold-dev/batcher and the relevant functions in the maths library https://github.com/ligolang/math-lib-cameligo/ with commit "03336655f036152ab2e98d6187376d010ff635cc".

Our reassessment considered commit "96c75a7bcb532eb34030d72aa447b4d60fd641bf" for Batcher DEX and "8b9368b7bf679b60f5158238bf8b38f92680361e" for the maths library. Furthermore, the following compiled smart contract was considered too:

- KT1CoTu4CXcWoVk69Ukbgwx2iDK7ZA4FMSpJ on Tezos mainnet

Scope limitations

Our security assessment is based on the following key assumptions and scope limitations:

- Any potential adversarial activities conducted by the administrator of the contract or operational errors by administrators were out of scope.
- Content of metadata and token metadata were out of scope. For instance, any off-chain views have not been assessed.
- The economic model of Batcher DEX, including the appropriate settings for thresholds, factors, constants, etc. was out of scope.
- The Oracle solution providing the matching prices was not in scope.

Methodology

Inference's methodology for smart contract security assessments on Tezos is a combination of a source code review of the smart contract source code in the high-level language (e.g. Ligo or SmartPy), and the resulting compiled code in Michelson. This approach provides additional assurance that the compiler producing the Michelson code is correct, and does not introduce any security issues. Furthermore, this approach fosters a better understanding for smart contract users of what has been reviewed and what has been effectively deployed on-chain.

In order to ensure a high quality in our security assessments, Inference is using subject matter experts having a high adversarial scenario mindset to spot potential issues in smart contracts under review. Additionally, we apply checklists derived from good practices and commonly known issues based on the Tezos smart contract assessment checklist to document our work and to ensure good issue coverage.

Furthermore, Inference maintains regular communications with the smart contract development team to ensure a correct understanding of the smart contract solution and environment, but also to make teams aware of any observations as soon as possible.

Inference's internal quality assurance procedures ensure that results of security assessments are challenged for completeness and appropriateness by a second independent expert.

Objectives

The objectives are the identification of security issues with regards to the assessed smart contracts and their conceptual design and specification. The security assessment also focuses on adversarial scenarios on specific use cases which have been listed in the appendix named Adversarial scenarios. These were identified together with the tzConnect's FA2 smart contract template developers and checked during our security assessment.

Activities

Our activities for the initial assessment and for the defined scope were:

- Source code review of smart contract code in Ligo

We applied the checklist for smart contract security assessments on Tezos, version 1.2 obtained from https://github.com/InferenceAG/TezosSecurityAssessmentChecklist. We applied the following security checklist tables:

- System / Platform
- Storage
- Gas issues and efficiency
- Code issues
- Transaction
- Entrypoint
- Admin / Operator functions
- Other topics & test cases

Our activities for the reassessment were:

- Source code review of changes in the smart contract code in Ligo,
- Source code review of changes in the deployed smart contract in Michelson on mainnet and
- Reassessing security issues and observations from the initial assessment if claimed to be resolved.

Security issues

There are no open known security issues.

Observations

O-MBA-001: Use of appropriate tokens

The redeem entrypoint will leave minimal amounts (“dust”) of swapped tokens in the custody of the Batcher DEX smart contract.

It is therefore crucial that only appropriate token smart contracts are added to Batcher DEX. Token smart contracts should have enough decimals so that any potential leftovers have a small real value.

Since only Batcher DEX admins can add new token pairs / tokens, we raise this issue only as an observation in this report.

Recommendation:
We recommend analysing the situation and potentially considering measures such as providing clear documentation and guidelines for admins on the required characteristics of the reward token smart contract.

Comment from Marigold:
Code has been updated to ensure tokens have a minimal 6 decimals precision.

Results from follow-up assessment:
We updated the status from “open” to “partially closed” in order to raise awareness of this situation to potential admins of the Batcher DEX, since even 6 decimals could be too low depending on the design and characteristics of the token.

Disclaimer

This security assessment report ("Report") by Inference AG ("Inference") is solely intended for Marigold ("Client") with respect to the Report's purpose as agreed by the Client. The Report may not be relied upon by any other party than the Client and may only be distributed to a third party or published with the Client's consent. If the Report is published or distributed by the Client or Inference (with the Client's approval) then it is for information purposes only and Inference does not accept or assume any responsibility or liability for any other purpose or to any other party.

Security assessments of a software or technology cannot uncover all existing vulnerabilities. Even an assessment in which no weaknesses are found is not a guarantee of a secure system. Generally, code assessments enable the discovery of vulnerabilities that were overlooked during development and show areas where additional security measures are necessary. Within the Client's defined time frame and engagement, Inference has performed an assessment in order to discover as many vulnerabilities of the technology or software analysed as possible. The focus of the Report's security assessment was limited to the general items and code parts defined by the Client. The assessment shall reduce risks for the Client but in no way claims any guarantee of security or functionality of the technology or software that Inference agreed to assess. As a result, the Report does not provide any warranty or guarantee regarding the defect-free or vulnerability-free nature of the technology or software analysed.

In addition, the Report only addresses the issues of the system and software at the time the Report was produced. The Client should be aware that blockchain technology and cryptographic assets present a high level of ongoing risk. Given the fact that inherent limitations, errors or failures in any software development process and software product exist, it is possible that even major failures or malfunctions remain undetected by the Report. Inference did not assess the underlying third party infrastructure which adds further risks. Inference relied on the correct performance and execution of the included third party technology itself.

Appendix

Adversarial scenarios

The following adversarial scenarios have been identified together with Marigold's Batcher DEX smart contract developers and checked during our security assessment.

Scenario	Assessment result
Extracting assets by unauthorised parties.	**Ok** Nothing identified.
Batcher DEX users extract more assets than allowed.	**Ok** Nothing identified.
Influencing the matching price.	**Not assessed:** The Oracle solution was not in scope of this assessment. **Note:** Depending on how often the Oracle prices are provided and how Batcher DEX's constants are set, the matching price still can not be influenced, but may be already known short before the deposit window ends. This may lead to an advantage for users which are depositing late.

Risk rating definition for smart contracts

Severities are quantified with two dimensions, roughly defined as follows, whereas the examples have to be regarded as indication only:

Probability of occurrence / materialisation of an issue
(bullets for a category are linked with each other with “and/or” condition.)

- Low:
  - A trusted / privileged role is required.
  - Contract may end up in the issue if other conditions, which are also unlikely to happen, are required.
- Medium:
  - A specific role or contract state is required to trigger the issue.
  - Contract may end up in the issue if another condition is fulfilled as well.
- High:
  - Anybody can trigger the issue.
  - Contract’s state will over the short or long term end up in the issue.

Impact:
(bullets for a category are linked with each other with “and/or” condition.)

- Low:
  - Non-compliance with TZIP standards
  - Unclear error messages
  - Confusing structures
- Medium:
  - A minor amount of assets can be withdrawn or destroyed.
- High:
  - Not inline with the specification
  - A non-minor amount of assets can be withdrawn or destroyed.
  - Entire or part of the contract becomes unusable.

Severity:

	Low impact	Medium impact	High impact
High probability	**High**	**Critical**	**Critical**
Medium probability	**Medium**	**High**	**Critical**
Low probability	**Low**	**Medium**	**High**

Glossary

Term	Description
Archetype	High level smart contract language. Website: https://archetype-lang.org/
Ligo	High level smart contract language. Website: https://ligolang.org/
Origination	Deployment of a smart contract
SmartPy	High level smart contract language. Website: https://smartpy.io/
TZIP	Tezos Improvement Proposal