



DeXe Platform Native Currency Update Diff Code Audit And Verification by Ambisafe Inc.

May 2024

Oleksii Matiasevych

1. **INTRODUCTION.** DeXe Network requested Ambisafe to perform a code audit of the DeXe Platform updated contracts. The code in question can be identified by the following git commit hash diff:

```
7d1daefbd11564f6c3caa080fcd6d90d216c7db2
...
dac37d017570c01e8944d1b4c77ebc3cdeccfa9a
```

All contracts in the repo are in scope.

After the initial code audit, DeXe Network team applied a number of updates which can be identified by the following git commit hash:

```
fb38f8ad96f662156d3cb5f7bca8b36524253ae8
```

Additional verification was performed after that.

2. **DISCLAIMER.** The code audit makes no statements or warranties about utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about fitness of the contracts for any specific purpose, or their bugfree status. The code audit documentation below is for internal management discussion purposes only and should not be used or relied upon by external parties without the express written consent of Ambisafe.
3. **EXECUTIVE SUMMARY.** There are **no** known compiler bugs for the specified compiler version (0.8.20), that might affect the contracts' logic. There were 0 critical, 0 major, 3 minor, 0 informational and optimizational findings identified in the initial version of the contracts. All the findings were addressed and were not found in the final version of the code.

4. **CRITICAL BUGS AND VULNERABILITIES.** No critical issues were identified.
5. **INITIAL LINE BY LINE REVIEW. FIXED FINDINGS.**
 - 5.1. GovPool, line 279. Minor, the **delegateTreasury()** function should execute **_lockBlock()** function on **delegatee** instead of a **msg.sender**.
 - 5.2. GovPool, line 343. Minor, the **undelegateTreasury()** function should execute **_checkBlock()** function on **delegatee** instead of a **msg.sender**.
 - 5.3. INetworkProperties, line 7. Minor, the **getNativeSupply()** function and the native amounts across the code base implicitly assume 18 decimals, even though some chains could have a different value.



Oleksii Matiasevych