CERTIK

CertiK Audit Report for Golem

Contents

Disclaimer

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 Verification Services Agreement between CertiK and Golem (the "Company"), or the scope of services/verification, and terms and conditions provided to the Company in connection with the verification (collectively, 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 without CertiK's prior written consent.

About CertiK

CertiK is a technology-led blockchain security company founded by Computer Science professors from Yale University and Columbia University built to prove the security and correctness of smart contracts and blockchain protocols.

CertiK, in partnership with grants from IBM and the Ethereum Foundation, has developed a proprietary Formal Verification technology to apply rigorous and complete mathematical reasoning against code. This process ensures algorithms, protocols, and business functionalities are secured and working as intended across all platforms.

CertiK differs from traditional testing approaches by employing Formal Verification to mathematically prove blockchain ecosystem and smart contracts are hacker-resistant and bug-free. CertiK uses this industry-leading technology together with standardized test suites,

static analysis, and expert manual review to create a full-stack solution for our partners across the blockchain world to secure 6.2B in assets. For more information: https://certik.org.

Executive Summary

We have audited the intended migration process of the Golem Network Token on the smart contract level. No major nor minor vulnerabilities have been found during this Audit.

Testing Summary

SECURITY LEVEL

Smart Contract Audits

This report has been prepared as a product of the Smart Contract Audit request by Golem Network. This audit was conducted to discover issues and vulnerabilities in the source code of Golem's New GNT Token and MigrationProxy Smart Contracts.

TYPE	Token
SOURCE CODE	https://github.com/golemfactory/gnt2/tree/master/gnt2-contracts/src/contracts/GNT2
PLATFORM	EVM
LANGUAGE	Solidity
REPORT DATE	Aug 22, 2020
METHODS	Static Analysis, Dynamic Analysis, and Manual Review, a comprehensive examination has been performed.

Scope of work

The files that were audited, were:

- *BatchingSidecar.sol*,
- *GNTMigrationAgent.sol* and
- *NewGolemNetworkToken.sol*,

Additionally, the *migrate* function in *GolemNetworkToken* in *Token.sol* (currently deployed).

The repo audited:

- https://github.com/golemfactory/gnt2/tree/master/gnt2-contracts/src/contracts/GNT2

The commit hash that was audited, and the commit hash that all line references refer to, is:

- **922728b63db7664a4a61051ae28fee506b95992f**

Review Notes

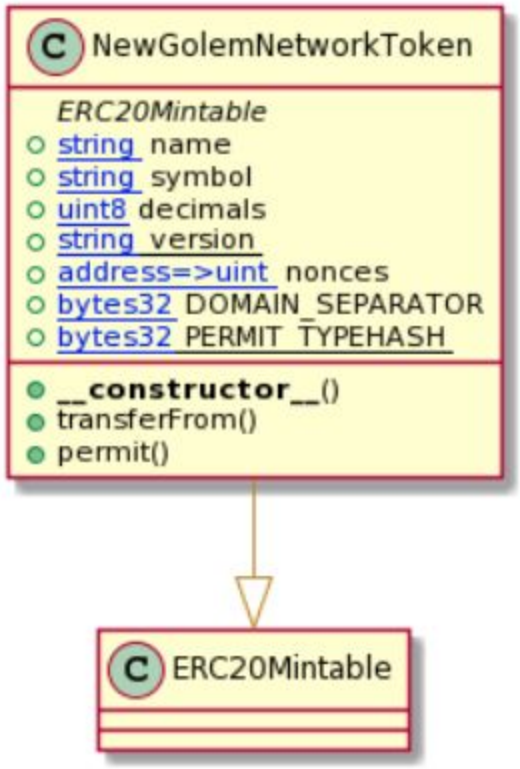
Items are labeled [CRITICAL], [MAJOR], [MINOR], [INFO], [DISCUSSION] (in decreasing significance).

Review Findings

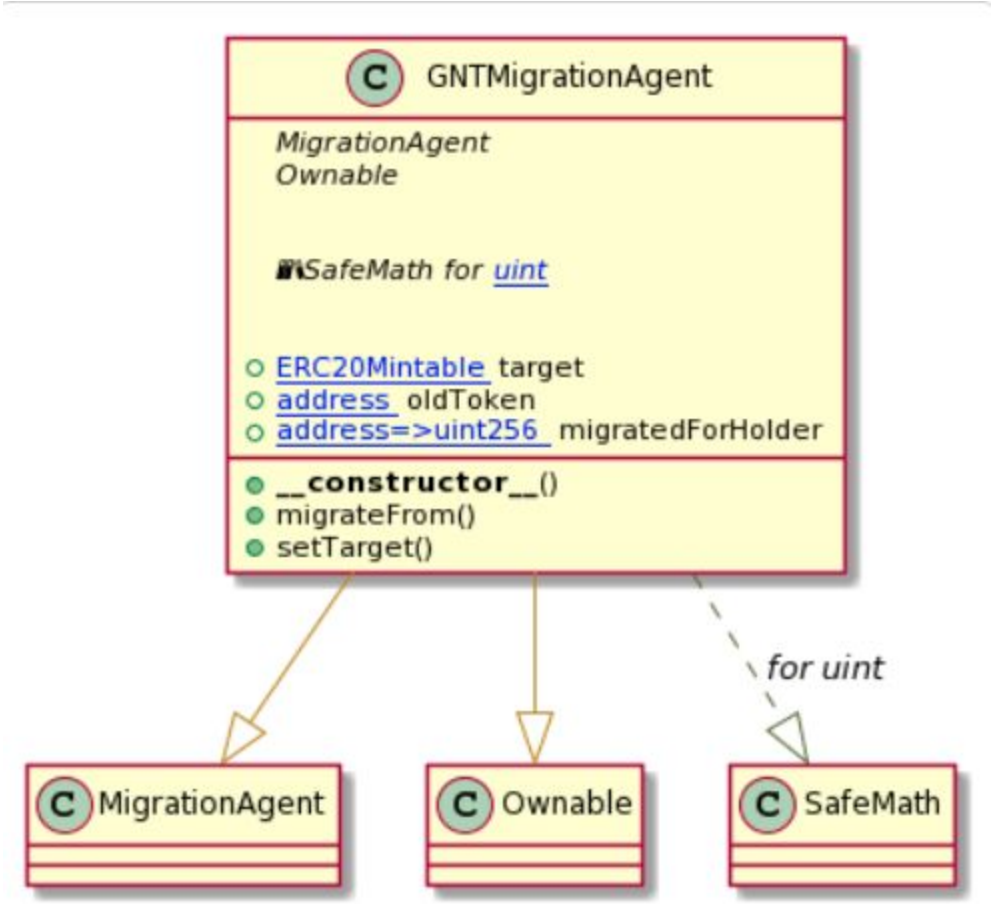
1. [DISCUSSION] The batching sidecar functionality could be implemented directly in the new GNT.

2. [DISCUSSION] The owner of GNTMigrationAgent has power over the migration process. They may for example migrate their own tokens, then set the target to one that would revert on a `.mint` CALL, meaning nobody else will be able to migrate. We don't see any easy fix to this, implying that this is necessary to facilitate the migration at least in the short-term. It should also be noted that once a sufficiently long period has passed (i.e. every old token holder has been given the chance to migrate), then either changing the target and renouncing ownership (in GNTMigrationAgent), or renouncing mintership (in NewGolemNetworkToken) will renounce these elevated powers.

Appendix: NewGolemNetworkToken



Appendix: GNTMigrationAgent



Appendix: Batching Sidecar