CHAINSECURITY

August 15th 2019

Digital Gold Ltd
Suite 305, Griffith Corporate Centre,
P.O. Box 1510, Beachmont Kingstown,
St. Vincent and the Grenadines

Statement of Security Code Audit

ChainSecurity was tasked by Digital Gold with an audit of their Gold.Storage smart contracts. In the following we describe the project and the findings of the audit.

The smart contracts include an ERC20-compatible token with the following details: (1) Name: Gold Storage, (2) Symbol: GOLD, (3) Decimals: 3. The token is ownable and the contract owner can mint and burn tokens from and to accounts. Users can also burn their token if desired. Additionally, to the standard ERC20 token features the token implements the option to charge transfer fees and holding fees. These fees vary depending on whether or not the user has the partner status. Fractions of a fee are rounded up. The transfer fees are deducted when a transfer occurs. The holding fees are deducted in so called burnouts. To partially pay for the gas costs of a burnout, Digital Gold implements a gas-collection system in a GasTank library. This library mints gas tokens each time a user transfers tokens.

Blockchain projects rely on the detailed public audits by ChainSecurity to ensure top-grade security for their smart contracts and protocols. ChainSecurity conducted a thorough code audit to certify the security of the project. The audit process consisted of a manual and automated code audit, checking for potential security issues, and reviewing the project's design and architecture for compliance with best practices. To deliver the highest assurance guarantees for the project, ChainSecurity used state-of-the-art analysis tools based on the latest research from ETH Zurich, one of the best technical universities.

During the code audit, ChainSecurity identified two medium and three low severity issues. All discovered issues were addressed or acknowledged. If key and contract management are performed correctly by the contract owner, Chainsecurity sees no remaining security issues.

The following files (with the corresponding SHA-256 hashes) were audited:

File	SHA-256 hash
ERC20Interface.sol :	62fe71d8ce8e6708a219802d421245bf7701135d65deb6f90d26491a30212587
GasTank.sol :	f60013e1ca2497eed52ad588b0d72f589cebbb0d9c8b0e1399a45a66ba2a2a7f
GoldStorage.sol :	ce965e42a433cf1aa13b4a4dd0eea6f72316c81604e9e0c35bdebe0d08206c46
Graceful.sol :	3f3ebc399ff9347cea4d112ac0852b1bb1a7269b569477b336282a07491976b1
Owned.sol :	d7735c056d4dd2efa258cd8191ceef9b9f9a534b657b3341e3aec65f79fd3461

CHAINSECURITY