Anthem Gold

Contract Audit

REPORT DATE	March 10th, 2019
REPORT VERSION	1.0

PREPARED BY

HOSHO

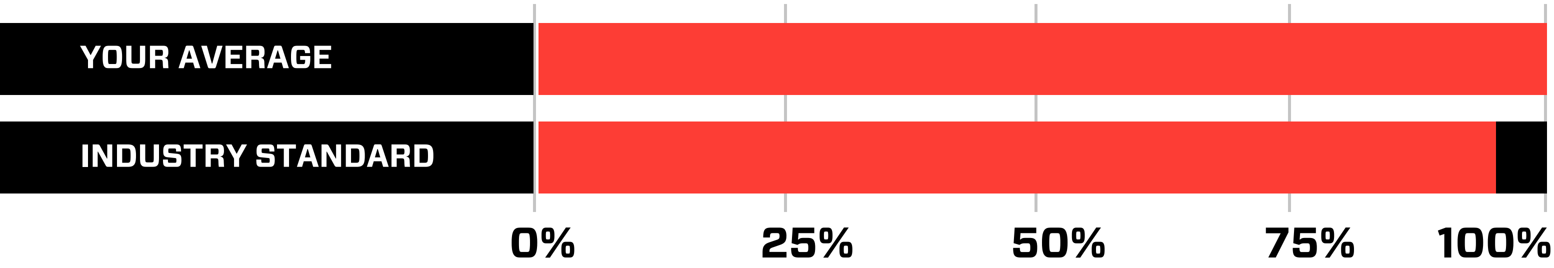
Executive Summary

This document outlines the overall security of AnthemGold's smart contract as evaluated by Hosho's Smart Contract auditing team. The scope of this audit was to analyze and document AnthemGold's token contract codebase for quality, security, and correctness.

Contract Status

No issues were discovered in this contract during the auditing process. (See Complete Analysis)

Testable Code



Testable code is 100.00%, which is above the industry standard of 95%. (See Coverage Report)

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that's able to withstand the Ethereum network's fast-paced and rapidly changing environment, we at Hosho recommend that the AnthemGold team put in place a bug bounty program to encourage further and active analysis of the smart contract.

Table of Contents

Auditing Strategy and Techniques Applied

The Hosho team has performed a thorough review of the smart contract code, the latest version as written and updated on February 6th, 2018. All main contract files were reviewed using the following tools and processes. (See All Files Covered)

Throughout the review process, care was taken to ensure that the token contract:

- Implements and adheres to existing ERC-20 Token standards appropriately and effectively;
- Documentation and code comments match logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices in efficient use of gas, without unnecessary waste;
- Uses methods safe from reentrance attacks; and
- Is not affected by the latest vulnerabilities.

The Hosho team has followed best practices and industry-standard techniques to verify the implementation of AnthemGold's token contract. To do so, the code is reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as they are discovered. Part of this work includes writing a unit test suite using the Meadow testing framework. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

1 **Due diligence in assessing the overall code quality of the codebase.**

2 **Cross-comparison with other, similar smart contracts by industry leaders.**

3 **Testing contract logic against common and uncommon attack vectors.**

4 **Thorough, manual review of the codebase, line-by-line.**

5 **Deploying the smart contract to testnet and production networks using multiple client. implementations to run live tests.**

2.1 Summary

The AnthemGold contracts form an ERC-20 token with mint, pause, blacklist, and transfer functionality. The contracts properly implement the ERC-20 standards, make use of an ownership system, and utilize burnable functionality to dispose of tokens when needed.

2.2 Coverage Report

As part of our work assisting AnthemGold in verifying the correctness of their contract code, our team was responsible for writing a unit test suite using the Meadow testing framework.

- Branches: 100%
- Functions: 100%
- Lines: 100%

2.3 Failing Tests

No failing tests!

Complete Analysis

For ease of navigation, sections are arranged from most critical to least critical. Issues are tagged “Resolved” or “Unresolved” depending on whether they have been fixed or still need addressing. Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

● Critical

The issue affects the contract in such a way that funds may be lost, allocated incorrectly, or otherwise result in a significant loss.

● High

The issue affects the ability of the contract to compile or operate in a significant way.

● Medium

The issue affects the ability of the contract to compile or operate in a significant way.

● Low

The issue has minimal impact on the contract’s ability to operate.

● Informational

The issue has no impact on the contract’s ability to operate, and is meant only as additional information.

3.1 Resolved: Single-Step Ownership Transfer

INFORMATIONAL

Contract: Ownable

Explanation

The implementation of Ownership in the AnthemGold token contracts allows the contract owner to unilaterally and instantly transfer ownership to another Ethereum address, with no path for recovery in the case of a bad ownership transfer (i.e. a typo). It is considered best practice to ensure that all ownership transfers are first proposed by the current owner, then either accepted by the new owner or canceled by the current owner. This allows for ownership transfers to incorrect addresses to be canceled, and the correct transfer executed, without permanently risking the ability to control the contract.

Update

AnthemGold has acknowledged and accepted the risks surrounding this informational issue.

We are grateful to have been given the opportunity to work with the AnthemGold team.

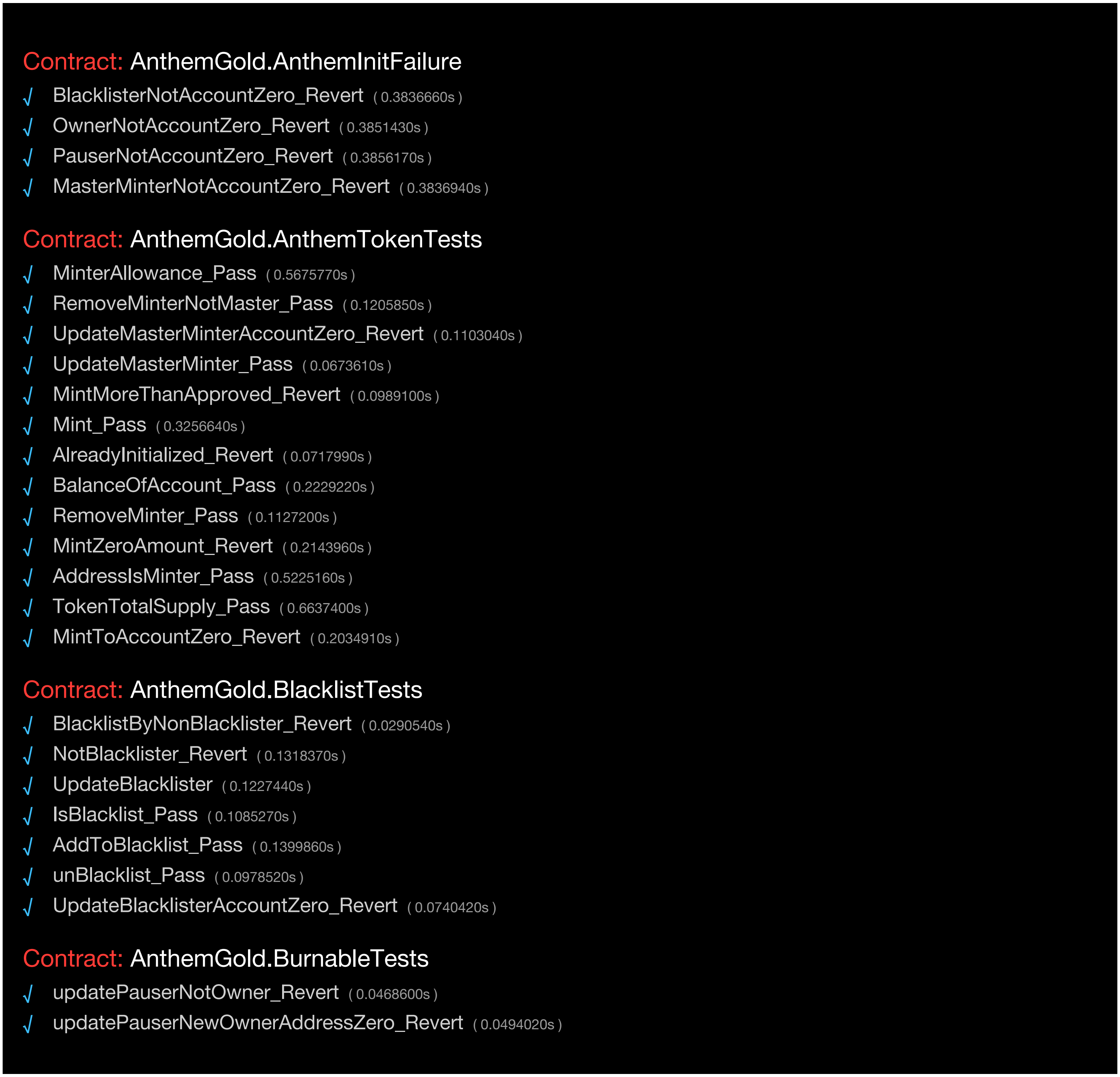
The AnthemGold contracts implement a complete ERC-20 token solution. No issues or vulnerabilities were found during Hosho's assessment, and the contracts have passed Hosho's auditing process.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them.

We at Hosho recommend that the AnthemGold team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

HOSHO

Test Suite Results



```
Contract: AnthemGold.AnthemInitFailure
√  BlacklisterNotAccountZero_Revert  ( 0.38366660s )
√  OwnerNotAccountZero_Revert  ( 0.3851430s )
√  PauserNotAccountZero_Revert  ( 0.3856170s )
√  MasterMinterNotAccountZero_Revert  ( 0.3836940s )

Contract: AnthemGold.AnthemTokenTests
√  MinterAllowance_Pass  ( 0.5675770s )
√  RemoveMinterNotMaster_Pass  ( 0.1205850s )
√  UpdateMasterMinterAccountZero_Revert  ( 0.1103040s )
√  UpdateMasterMinter_Pass  ( 0.0673610s )
√  MintMoreThanApproved_Revert  ( 0.0989100s )
√  Mint_Pass  ( 0.3256640s )
√  AlreadyInitialized_Revert  ( 0.0717990s )
√  BalanceOfAccount_Pass  ( 0.2229220s )
√  RemoveMinter_Pass  ( 0.1127200s )
√  MintZeroAmount_Revert  ( 0.2143960s )
√  AddressIsMinter_Pass  ( 0.5225160s )
√  TokenTotalSupply_Pass  ( 0.6637400s )
√  MintToAccountZero_Revert  ( 0.2034910s )

Contract: AnthemGold.BlacklistTests
√  BlacklistByNonBlacklister_Revert  ( 0.0290540s )
√  NotBlacklister_Revert  ( 0.1318370s )
√  UpdateBlacklister  ( 0.1227440s )
√  IsBlacklist_Pass  ( 0.1085270s )
√  AddToBlacklist_Pass  ( 0.1399860s )
√  unBlacklist_Pass  ( 0.0978520s )
√  UpdateBlacklisterAccountZero_Revert  ( 0.0740420s )

Contract: AnthemGold.BurnableTests
√  updatePauserNotOwner_Revert  ( 0.0468600s )
√  updatePauserNewOwnerAddressZero_Revert  ( 0.0494020s )
```

Appendix A

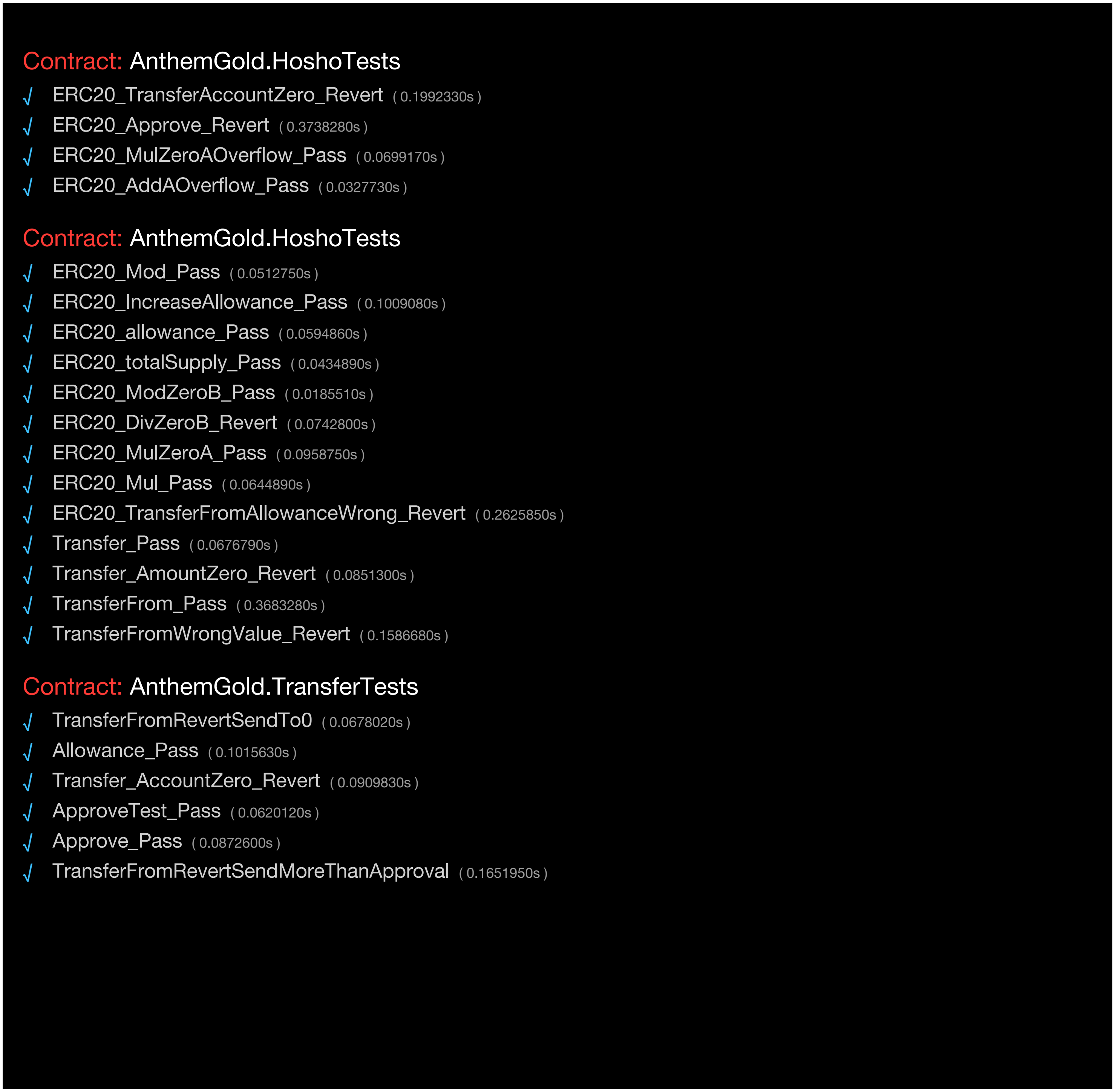
```
Contract: AnthemGold.BurnableTests
√  updatePauser_Pass  ( 0.0496760s )
√  pauseAndUnpauseByPauser_Pass  ( 0.0800620s )
√  Burnable_noBalance_Revert  ( 0.0334220s )
√  transferOwnershipNewOwnerAddressZero_Revert  ( 0.0478010s )

Contract: AnthemGold.BurnableTests
√  transferOwnership_Pass  ( 0.0749940s )
√  UnpauseByNonPauser_Revert  ( 0.0341490s )
√  WhenNotPaused_Modifier_Revert  ( 0.0914190s )
√  Burnable_burn_burnsTokens  ( 0.1615650s )
√  OnlyMinters_Modifier_Revert  ( 0.0509000s )
√  pauseByNonPauser_Revert  ( 0.1212650s )
√  transferOwnershipNotOwner_Revert  ( 0.0724710s )
√  Burnable_noAmount_Revert  ( 0.0573830s )
√  ERC20_DecreaseAllowance_Pass  ( 0.0789200s )
√  ERC20_TransferFromAccountZero_Revert  ( 0.2698870s )
√  ERC20_Transfer_Pass  ( 0.2541990s )
√  ERC20_ApproveSpenderAccountZero_Revert  ( 0.0568540s )
√  ERC20_Approve_Pass  ( 0.0574090s )

Contract: AnthemGold.HoshoTests
√  ERC20_Div_Pass  ( 0.0888880s )
√  ERC20_BurnFrom_Pass  ( 0.1905160s )
√  ERC20_Burn_Pass  ( 0.1972520s )
√  ERC20_TransferFrom_Pass  ( 0.2827190s )
√  ERC20_IncreaseAllowanceAccountZero_Revert  ( 0.1322810s )
√  BalanceOf_TotalSupply_Approve  ( 0.0972530s )
√  ERC20_DecreaseAllowanceAccountZero_Revert  ( 0.0801130s )

Contract: AnthemGold.HoshoTests
√  ERC20_MintAccountZero_Revert  ( 0.0729020s )
√  ERC20_BurnAccountZero_Revert  ( 0.1196290s )
```

Appendix A



```
Contract: AnthemGold.HoshoTests
√  ERC20_TransferAccountZero_Revert  ( 0.1992330s )
√  ERC20_Approve_Revert  ( 0.3738280s )
√  ERC20_MulZeroAOverflow_Pass  ( 0.0699170s )
√  ERC20_AddAOverflow_Pass  ( 0.0327730s )

Contract: AnthemGold.HoshoTests
√  ERC20_Mod_Pass  ( 0.0512750s )
√  ERC20_IncreaseAllowance_Pass  ( 0.1009080s )
√  ERC20_allowance_Pass  ( 0.0594860s )
√  ERC20_totalSupply_Pass  ( 0.0434890s )
√  ERC20_ModZeroB_Pass  ( 0.0185510s )
√  ERC20_DivZeroB_Revert  ( 0.0742800s )
√  ERC20_MulZeroA_Pass  ( 0.0958750s )
√  ERC20_Mul_Pass  ( 0.0644890s )
√  ERC20_TransferFromAllowanceWrong_Revert  ( 0.2625850s )
√  Transfer_Pass  ( 0.0676790s )
√  Transfer_AmountZero_Revert  ( 0.0851300s )
√  TransferFrom_Pass  ( 0.3683280s )
√  TransferFromWrongValue_Revert  ( 0.1586680s )

Contract: AnthemGold.TransferTests
√  TransferFromRevertSendTo0  ( 0.0678020s )
√  Allowance_Pass  ( 0.1015630s )
√  Transfer_AccountZero_Revert  ( 0.0909830s )
√  ApproveTest_Pass  ( 0.0620120s )
√  Approve_Pass  ( 0.0872600s )
√  TransferFromRevertSendMoreThanApproval  ( 0.1651950s )
```

Appendix B

FILE	FINGERPRINT
AGLDTokenV1.sol	AF50045C12ACA3D823DAF497B3A6F29BB8EE8421DB2BA3A707273994098D9B70
AGLDTokenV2.sol	1805F460C0DD11A47BEB29464BA7EEAFE24E68E63F8A1A63D946ABD354D53283
Blacklistable.sol	C33A68CF46A4139B47114E0982903292CB17DBA5DC9BF8F2368C60D4425164C1
ERC20.sol	2D812BEEECE0CF4C83DC9B89E011EB9BFC07195D670D20E9FA519B12156B505F
IERC20.sol	103F9AE7C0715BB0E07F1258958A2C34E78800D49C877C0082FEF0763CE1A576
Ownable.sol	413332CFEA8F4B8411A496E9741757ACB411550AFEDA244C29519807A6492305
Pausable.sol	8D16ADFE875594758DC1CBE753D81F949C883EBB67047299EC9BD154B40D5A45

Appendix C

FILE	% BRANCHES	% FUNCTION	% LINES
AGLDTokenV1.sol	100%	100%	100%
AGLDTokenV2.sol	100%	100%	100%
Blacklistable.sol	100%	100%	100%
ERC20.sol	100%	100%	100%
IERC20.sol	100%	100%	100%
Ownable.sol	100%	100%	100%
Pausable.sol	100%	100%	100%
ALL FILES	100%* (76/76)	100%* (42/42)	100%* (152/152)

* Totals are calculated using weighted percentages