Blockwell Smart Contract Audit

Date: 30 October 2019

QASH

Audit Process: This audit was performed as a three prong security and token stability audit involving**:**

1) Static Analysis: In-depth, line by line reading of the code, modeling, and best practice verification.

2) Real World Testing: Replicating and re-launching of the token on an ethereum based Testnet for hands in manual testing and verification.

3) Blockwell Khaleesi: The "breaker of chains", our token test automation suite which loads a copy of the token and attacks it as a hacker's "attack bot" would.

Each step is meant to catch flaws, highlight critical vulnerabilities and provide redundancy so we can provide the quality bar our clients, platform users and partners trust us to.

Audit Summary: The QASH Token has **passed** the smart contract audit. With our audit of their smart contract source code we assert that the contracts are in good status based on current knowledge of Solidity flaws, automated testing, linting, and line by line analysis.

Assessment: PASSED

Report: Based on review, we believe there are no critical technical concerns with the contract launching on mainnet and these tokens trading.

The only potential improvements to the contract discovered were minor redundancies in checking for allowed and balances twice due to SafeMath duplicating the check, which leads to a very small increase in gas use.

Function call tests (PASSED)

Basic transfer to second account

Basic test of the transfer function.

Pass

`function transfer(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D, 100)`

Events

Transfer(0xf20318e973cbf60669151c1b3d633793970ec90d, 0x03638f1f1aa4796f8746acd39f8bcc15c872e86d, 100)

Transfer too much

Test attempting to transfer more tokens than the sender's balance.

Pass

`function transfer(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D, 100000000000000000000000000)`

Transfer maximum

Test transfering the maximum value of uint256 for potential overflow issues.

Pass

`function transfer(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D,`
`115792089237316195423570985008687907853269984665640564039457584007913129639935)`

Transfer from, without approval

Test using transferFrom without being approved.

Pass

`function transferFrom(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D,`
`0xf20318e973CbF60669151C1B3d633793970eC90D, 2)`

Approve

Basic test of the approve function.

Pass

`function approve(0xf20318e973CbF60669151C1B3d633793970eC90D, 100)`

Events

Approval(0x03638f1f1aa4796f8746acd39f8bcc15c872e86d, 0xf20318e973cbf60669151c1b3d633793970ec90d, 100)

Basic transfer from

Basic test of the transferFrom function.

Pass

`function transferFrom(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D,`
`0xf20318e973CbF60669151C1B3d633793970eC90D, 2)`

Events

Transfer(0x03638f1f1aa4796f8746acd39f8bcc15c872e86d, 0xf20318e973cbf60669151c1b3d633793970ec90d, 2)

Transfer from, higher than balance

Test transfering an approved amount that's higher than the source account's balance.

Pass

```
function transferFrom(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D,
0xf20318e973CbF60669151C1B3d633793970eC90D, 150)
```

Change approval

Test changing approval to a lower value.

Pass

```
function approve(0xf20318e973CbF60669151C1B3d633793970eC90D, 2)
```

Events

Approval(0x03638f1f1aa4796f8746acd39f8bcc15c872e86d, 0xf20318e973cbf60669151c1b3d633793970ec90d, 2)

Transfer from, more than approval

Test transferFrom that's below the previous approval amount, but above the new approval amount.

Pass

```
function transferFrom(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D,
0xf20318e973CbF60669151C1B3d633793970eC90D, 3)
```

Transfer from, remaining approval

Transfer the from account's remaining approved balance and check that approval is now zero.

Pass

```
function transferFrom(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D,
0xf20318e973CbF60669151C1B3d633793970eC90D, 2)
```

Events

Transfer(0x03638f1f1aa4796f8746acd39f8bcc15c872e86d, 0xf20318e973cbf60669151c1b3d633793970ec90d, 2)

Transfer from, approval depleted

Test transferFrom with approval depleted.

Pass

```
function transferFrom(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D,
0xf20318e973CbF60669151C1B3d633793970eC90D, 2)
```

Pause token transfers

Basic test of pausing transfers.

Pass

`function pause()`

Events

Paused(0xf20318e973cbf60669151c1b3d633793970ec90d, false)

Test token pausing

Test token transfer after pausing to ensure it works correctly.

Pass

`function transfer(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D, 100)`

Unpause token transfers

Basic test of unpausing transfers.

Pass

`function unpause()`

Events

Unpaused(0xf20318e973cbf60669151c1b3d633793970ec90d)

Test token unpausing

Test token transfer after unpausing to ensure it works correctly.

Pass

`function transfer(0x03638F1f1aa4796F8746Acd39F8BcC15c872E86D, 100)`

Events

Transfer(0xf20318e973cbf60669151c1b3d633793970ec90d, 0x03638f1f1aa4796f8746acd39f8bcc15c872e86d, 100)