Corion - CorionX Token

Quality assurance

Table of content

Introduction

This documentation summarizes some of the quality assurance metrics and measures that were
taken into consideration during the development and deployment of the token.
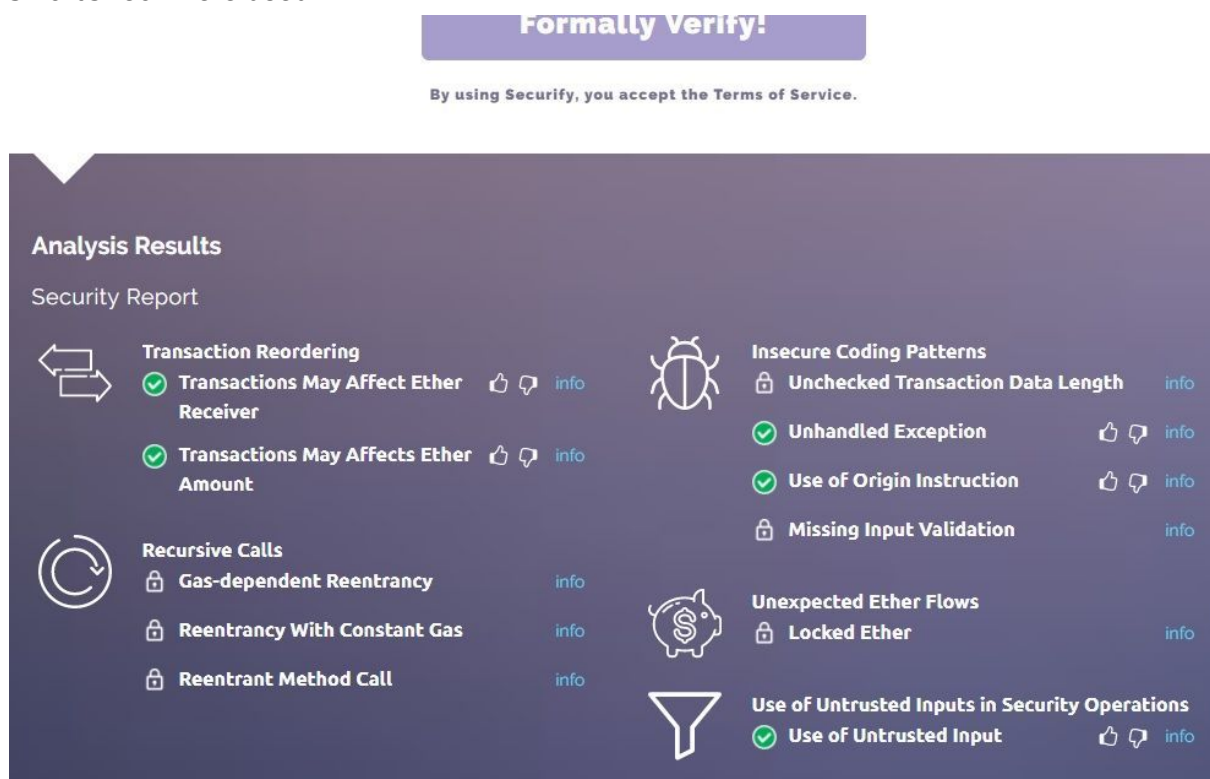
Code reuse

For most of the basic libraries standard libraries of the OpenZeppelin project were used.

Formal Code verification

Application

For formal source code verification two experimental tools, the free version of security and
SmartCheck were used.

Securify shows all green from the possible checks:

Smart Check

Smart Check identifies the following sev 1 - 4 findings:

Using the approve function of the ERC-20 standard

it is really an approve function of an ERC-20 token

No payable fallback function

the token is not planned to contain payment

Reentancy

Some parts of the code might be vulnerable to special reentrancy attacks. As the indicated code fragments are part of the OpenZeppelin project and the indicated severity is only 3, we consider the risk as low.

Visibility

some visibility were not defined explicitly however they were manually checked if they contain the correct values.

Delivery test

First delivery of the token to the rinkeby test network was analyzed and documented in details.

Please note that the tests and use-cases were initially with 8 decimals tested and initial supply 400 000 000 000 000.

Test parameters (ropsten)

TEST1	0x9b46BE2116F52f63B81bd98961efCDb4B0397540
TEST2	0x53cb49375f1A3f1331Cdf87054D73BBA08215634
MAIN	0x18921a0F96805AbAEF9ce33ee0fD653f15f88B7d
CONTRACT	0xe72f01A9d819C28C9b0A7c9cD6242224E5f73169

Youtube video list

https://www.youtube.com/playlist?list=PLs1AlTaVDA13odBE_TvxwejXpiowCeHOY

Checks after first deployment ethereum explorer

https://youtu.be/zKT6iazOSJ4

Balance of owner mist:

Deployed Contracts

CorionXToken at 0xe72...73169 (blockchain)

approve	address _spender, uint256 _value
decreaseApproval	address _spender, uint256 _subtractedValue
increaseApproval	address _spender, uint256 _addedValue
kill	
transfer	address _to, uint256 _value
transferFrom	address _from, address _to, uint256 _value
allowance	address _owner, address _spender
balanceOf	0x18921a0f96805abaef9ce33ee0fd653f15f88b7d

0: uint256: balance 40000000000000000

decimals

0: uint8: 8

INITIAL_SUPPLY

0: uint256: 40000000000000000

name

0: string: CorionX utility token

owner

0: address: 0x18921a0F96805AbAEF9ce33ee0fD653f15f88B7d

symbol

0: string: CORX

totalSupply

0: uint256: 40000000000000000

Token holder ethereum explorer

Token CorionX utility token ⓘ

Summary [ERC-20]

Total Supply:	400,000,000 CORX		Contract:	0xe72f01A9d819C28C9b0A7c9cD6242224E5f73169
Holders:	1 addresses		Decimals:	8
Transfers:	2		Links:	Not Available, Update ?
			Filtered By:	Enter Address/TxHash [Apply]

Transfers   Holders   ReadContract   Write Contract ᴮᵉᵗᵃ

🥧 TokenHolders Chart

A Total Of 1 Token Holder

First Prev Page 1 of 1 Next Last

Rank	Address	Quantity	Percentage
1	0x18921a0f96805abaef9ce33ee0fd653f15f88b7d	400000000	100.0000%

Transfer into a new account

Transaction 0x9cf380f4349840b0b0d4fe180b4ec0cde..

Overview   Event Logs (1)

Transaction Information ◐ ◑

[This is a Ropsten Testnet Transaction Only]

TxHash:
0x9cf380f4349840b0b0d4fe180b4ec0cde6ed64e55b2bdc9fa18de8585d188b6c

TxReceipt Status:
Success

Block Height:
4138694 (3 Block Confirmations)

TimeStamp:
46 secs ago (Sep-29-2018 04:43:45 PM +UTC)

From:
0x18921a0f96805abaef9ce33ee0fd653f15f88b7d

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ⊘

Tokens Transfered:
▸ From 0x18921a0f96805ab... To 0x9b46be2116f52f6... for 1 ERC-20 (CORX)

Value:
0 Ether ($0.00)

Gas Limit:
51748

Gas Used By Transaction:

New balances:

Summary [ERC-20]

Total Supply:	400,000,000 CORX
Holders:	2 addresses
Transfers:	-

Contract:	0xe72f01A9d819C28C9b0A7c9cD6242224E5f73169
Decimals:	8
Links:	Not Available, Update ?
Filtered By:	Enter Address/TxHash Apply

Transfers   Holders   ReadContract   Write Contract Beta

🥧 TokenHolders Chart

A Total Of 2 Token Holders

First Prev Page **1** of 1 Next Last

Rank	Address	Quantity	Percentag
1	0x18921a0f96805abaef9ce33ee0fd653f15f88b7d	399999999	100.0000%
2	0x9b46be2116f52f63b81bd98961efcdb4b0397540	1	0.0000%

Etherscan © 2018 () | Advertising | Donations 0x71c7656ec7ab88b098defb751b7401b5f6d8976f

Transferring more than balance: error expected

https://youtu.be/IoLSIWgf4UM

TxHash:
0xe03b59ca5905c42727c2956d75c832e84c6d1b315f0beaf2eba60fd00fa95843

TxReceipt Status:
Fail

Block Height:
4138708 (1 Block Confirmation)

TimeStamp:
42 secs ago (Sep-29-2018 04:47:17 PM +UTC)

From:
0x18921a0f96805abaef9ce33ee0fd653f15f88b7d

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ⚠

⌐ Warning! Error Encounter during Contract Execution [Reverted] ☺

⌐ ⚠ ERC-20 Token Transfer Error (Unable To Locate Corresponding Transfer Event Logs), Check with Sender. ⓘ

Value:
0 Ether ($0.00)

Gas Limit:
3000000

Gas Used By Transaction:
23978

Gas Price:
0.000000004 Ether (4 Gwei)

Actual Tx Cost/Fee:
0.000095912 Ether ($0.000000)

Nonce & {Position}:
4 | {32}

Input Data:

```
Function: transfer(address _to, uint256 _value) ***

MethodID: 0xa9059cbb
[0]:  0000000000000000000000009b46be2116f52f63b81bd98961efcdb4b0397540
[1]:  00000000000000000000000000000000000000000000000008e1bc9bf040000
```

View Input As ▾

Transfering the amount back

Transfers	Holders	ReadContract	Write Contract Beta

🔴 TokenHolders Chart

A Total Of 2 Token Holders

First | Prev | Page 1 of 1 | Next | Last

Rank	Address	Quantity	Percentag
1	0x18921a0f96805abaef9ce33ee0fd653f15f88b7d	399999998	100.0000%
2	0x9b46be2116f52f63b81bd98961efcdb4b0397540	2	0.0000%

transfer

_to: 0x18921a0f96805abaef9ce33ee0fd653f15f88b7d

_value: 200000000

transact

TxHash:
0x37a8ca3c19ed1ee21f219f3980216cac31fb959d4d77961b7e257df2869c06ed

Block Height:
(Pending)

Time Last Seen:
🕐 00 days 00 hr 00 min 08 secs ago (Sep-29-2018 06:04:17 PM)

From:
0x9b46be2116f52f63b81bd98961efcdb4b0397540

To:
0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169

Token Transfer:
▸ Pending Transfer to → 0x18921a0f96805ab... .For 2 ERC-20 (CorionX utility token)

Value:
0 Ether ($0.000000)

Gas Limit:
36748

Gas Used By Transaction:
Pending

Gas Price:
0.000000004 Ether (4 Gwei)

TxHash:
0x37a8ca3c19ed1ee21f219f3980216cac31fb959d4d77961b7e257df2869c06ed

TxReceipt Status:
Success

Block Height:
4139094 (4 Block Confirmations)

TimeStamp:
50 secs ago (Sep-29-2018 06:04:15 PM +UTC)

From:
0x9b46be2116f52f63b81bd98961efcdb4b0397540

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ⊘

Tokens Transfered:
▸ From 0x9b46be2116f52f6... To 0x18921a0f96805ab...for 2 ERC-20 (CORX)

Value:
0 Ether ($0.00)

Gas Limit:
36748

Gas Used By Transaction:
21748

Gas Price:
0.000000004 Ether (4 Gwei)

Actual Tx Cost/Fee:
0.000086992 Ether ($0.000000)

| balanceOf | 0x9b46be2116f52f63b81bd98961efcdb4b0397540 | ⌄ |

0: uint256: balance 0

| balanceOf | 0x18921a0f96805abaef9ce33ee0fd653f15f88b7d | ⌄ |

0: uint256: balance 40000000000000000000

Contract:	0xe72f01A9d819C28C9b0A7c9cD6242224E5f73169
Decimals:	8
Links:	Not Available, Update ?
Filtered By:	Enter Address/TxHash Apply

Transfers   Holders   ReadContract   Write Contract ^{Beta}

TokenHolders Chart

A Total Of 1 Token Holder

First Prev Page **1** of 1 Next Last

Rank	Address	Quantity	Percentage
1	0x18921a0f96805abaef9ce33ee0fd653f15f88b7d	400000000	100.0000%

Transfer from without approvement

https://youtu.be/t5tw-SvMhsA

transferFrom

_from:	0x9b46BE2116F52f63B81bd98961efCDb4B0397540
_to:	0x18921a0f96805abaef9ce33ee0fd653f15f88b7d
_value:	50000000

transact

TxReceipt Status:
Fail

Block Height:
4169421 (5 Block Confirmations)

Time Stamp:
53 secs ago (Oct-04-2018 01:01:08 PM +UTC)

From:
0x53cb49375f1a3f1331cdf87054d73bba08215634

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ⚠
Warning! Error Encounter during Contract Execution [Reverted] ☺

Value:
0 Ether ($0.00)

Gas Limit:
3000000

Gas Used By Transaction:
25678

Gas Price:
0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee:
0.000025678 Ether ($0.000000)

Nonce & {Position}:
1 | {23}

Approve transfer into test account

https://youtu.be/_qZSMcT_TIY

approve

_spender: 0x53cb49375f1A3f1331Cdf87054D73BBA08215634

_value: 10

transact

TxReceipt Status:
Success

Block Height:
4169518 (1 Block Confirmation)

TimeStamp:
31 secs ago (Oct-04-2018 01:37:45 PM +UTC)

From:
0x9b46be2116f52f63b81bd98961efcdb4b0397540

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ✓

Value:
0 Ether ($0.00)

Gas Limit:
45226

Gas Used By Transaction:
45226

Gas Price:
0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee:
0.000045226 Ether ($0.000000)

allowance

_owner: 0x9b46BE2116F52f63B81bd98961efCDb4B0397540

_spender: 0x53cb49375f1A3f1331Cdf87054D73BBA08215634

call

0: uint256: 10

Increase approvement

https://youtu.be/ZdjDzwV1Q1c

TxHash:
0xb8be805a969fea39c7f3a70c27012c6a0e822811ad860fa67654a34baf3d55cb

TxReceipt Status:
Success

Block Height:
4169535 (2 Block Confirmations)

TimeStamp:
25 secs ago (Oct-04-2018 01:48:21 PM +UTC)

From:
0x9b46be2116f52f63b81bd98961efcdb4b0397540

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ⊘

Value:
0 Ether ($0.00)

Gas Limit:
30226

Gas Used By Transaction:
30226

Gas Price:
0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee:
0.000030226 Ether ($0.000000)

Nonce & {Position}:
3 | {33}

Input Data:

```
Function: approve(address _spender, uint256 _value) ***

MethodID: 0x095ea7b3
[0]:  00000000000000000000000053cb49375f1a3f1331cdf87054d73bba08215634
[1]:  0000000000000000000000000000000000000000000000000000000000000014
```

View Input As ▾

---

allowance   ⌃

_owner: 0x9b46BE2116F52f63B81bd98961efCDb4B0397540

_spender: 0x53cb49375f1A3f1331Cdf87054D73BBA08215634

                                        ⇄   call

0: uint256: 20

Decrease approval

allowance

_owner: 0x9b46BE2116F52f63B81bd98961efCDb4B0397540

_spender: 0x53cb49375f1A3f1331Cdf87054D73BBA08215634

0: uint256: 20

approve

_spender: 0x53cb49375f1A3f1331Cdf87054D73BBA08215634

_value: 10

transact

TxHash:
0xc76f473cb966517064a0d5f593f6eb2f9756d4e9415a7752bb6c1055e45d49be

TxReceipt Status:
Success

Block Height:
4169537 (1 Block Confirmation)

TimeStamp:
3 mins ago (Oct-04-2018 01:48:30 PM +UTC)

From:
0x9b46be2116f52f63b81bd98961efcdb4b0397540

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ✓

Value:
0 Ether ($0.00)

Gas Limit:
30226

Gas Used By Transaction:
30226

Gas Price:
0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee:
0.000030226 Ether ($0.000000)

Nonce & {Position}:
4 | {38}

Input Data:

```
Function: approve(address _spender, uint256 _value) ***

MethodID: 0x095ea7b3
[0]:  00000000000000000000000053cb49375f1a3f1331cdf87054d73bba08215634
[1]:  000000000000000000000000000000000000000000000000000000000000000a
```

View Input As ▾

---

allowance

| _owner: | 0x9b46BE2116F52f63B81bd98961efCDb4B0397540 |
| _spender: | 0x53cb49375f1A3f1331Cdf87054D73BBA08215634 |

🗂   call

0: uint256: 10

Transfer from bigger than allowed

https://youtu.be/mgjlVPSddto

[This is a Ropsten **Testnet** Transaction Only]

TxHash:
0x724d2fb23bb9e068f0fb616dc26abcac8f60f398a56f1b374733e60bf83d6035

TxReceipt Status:
Fail

Block Height:
4169546 (1 Block Confirmation)

TimeStamp:
1 min ago (Oct-04-2018 01:54:27 PM +UTC)

From:
0x53cb49375f1a3f1331cdf87054d73bba08215634

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ⚠
⌐ Warning! Error Encounter during Contract Execution [**Reverted**] ☺

Value:
0 Ether ($0.00)

Gas Limit:
3000000

Gas Used By Transaction:
25486

Gas Price:
0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee:
0.000025486 Ether ($0.000000)

Nonce & {Position}:
2 | {7}

Input Data:

```
Function: transferFrom(address _from, address _to, uint256 _value) ***

MethodID: 0x23b872dd
[0]:   0000000000000000000000009b46be2116f52f63b81bd98961efcdb4b0397540
[1]:   00000000000000000000000018921a0f96805abaef9ce33ee0fd653f15f88b7d
[2]:   000000000000000000000000000000000000000000000000000000000000001e
```

View Input As ▾

TxHash:
0x724d2fb23bb9e068f0fb616dc26abcac8f60f398a56f1b374733e60bf83d6035

TxReceipt Status:
Fail

Block Height:
4169546 (1 Block Confirmation)

TimeStamp:
1 min ago (Oct-04-2018 01:54:27 PM +UTC)

From:
0x53cb49375f1a3f1331cdf87054d73bba08215634

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ⚠
└── Warning! Error Encounter during Contract Execution [Reverted] ⊗

Value:
0 Ether ($0.00)

Gas Limit:
3000000

Gas Used By Transaction:
25486

Gas Price:
0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee:
0.000025486 Ether ($0.000000)

Nonce & {Position}:
2 | {7}

Input Data:

```
Function: transferFrom(address _from, address _to, uint256 _value) ***

MethodID: 0x23b872dd
[0]:    0000000000000000000000009b46be2116f52f63b81bd98961efcdb4b0397540
[1]:    00000000000000000000000018921a0f96805abaef9ce33ee0fd653f15f88b7d
[2]:    000000000000000000000000000000000000000000000000000000000000001e
```

View Input As ▾

Transfer from allowed amount

https://youtu.be/nzDfPYDY-K8

TxHash:
0x092698234d542a28f1ce5e4e1afdaf31c67d019dc6ed4615733f30b1ec81d976

TxReceipt Status:
Success

Block Height:
4169552 (1 Block Confirmation)

TimeStamp:
43 secs ago (Oct-04-2018 01:58:18 PM +UTC)

From:
0x53cb49375f1a3f1331cdf87054d73bba08215634

To:
Contract 0xe72f01a9d819c28c9b0a7c9cd6242224e5f73169 ⊘

Tokens Transfered:
▸ From 0x9b46be2116f52f6... To 0x18921a0f96805ab...for 0.0000001 ERC-20 (CORX)

Value:
0 Ether ($0.00)

Gas Limit:
44122

Gas Used By Transaction:
29122

Gas Price:
0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee:

Contract:	0xe72f01A9d819C28C9b0A7c9cD6242224E5f73169
Decimals:	8
Links:	Not Available, Update ?
Filtered By:	Enter Address/TxHash Apply

Transfers   **Holders**   ReadContract   Write Contract ^{Beta}

A Total Of 2 Token Holders

First Prev Page **1** of **1** Next Last

Rank	Address	Quantity	Percentage
1	0x18921a0f96805abaef9ce33ee0fd653f15f88b7d	399999998.5	100.0000%
2	0x9b46be2116f52f63b81bd98961efcdb4b0397540	1.4999999	0.0000%