DIGITAL OCEAN

Security Assessment

Revolotto

Oct 5th, 2021

digitalocean.finance

Summary

This report has been prepared for Revolotto (RVL) to discover issues and vulnerabilities in the source code of the Revolotto (RVL) project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Testnet Deployment techniques.

The auditing process pays special attention to the following considerations:
Testing the smart contracts against both common and uncommon attack vectors.
Assessing the codebase to ensure compliance with current best practices and industry standards.
Ensuring contract logic meets the specifications and intentions of the client.
Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices.

We suggest recommendations that could better serve the project from the security perspective:
Enhance general coding practices for better structures of source codes;
Add enough unit tests to cover the possible use cases;
Provide more comments per each function for readability, especially contracts that are verified in public;
Provide more transparency on privileged activities once the protocol is live.

This is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below - please make sure to read it in full.

Overview

Digital Ocean was commissioned by Revolotto to perform an audit of smart contracts:

0x6dc3d0D6EC970BF5522611D8eFF127145D02b675

The purpose of the audit was to achieve the following:

Ensure that the smart contract functions as intended.
Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improving the security posture of the smart contract by remediating the issues that were identified.

Project Summary

Name	Revolotto
Description	Next-Gen Deflationary Four-Dimensional Revolutionary Lottery Coin. Revolotto is establishing the new standard of decentralized finance with its innovative coin circulation cycles, ultra burn protocol, and smart staking system.
Platform	BSC
Language	Solidity
Codebase	https://bit.ly/RevolottoContract
Website	https://www.revolotto.org

Contract Details

Contract Address	0x6dc3d0D6EC970BF5522611D8eFF127145D02b675
Total Supply	210,000,000 RVL
Symbol	RVL
Decimals	18
Liquidity Fee	9%
Reflection Fee	6%
Burn Fee	5%
Deployer Address	0x36fed7c1c2199bd8a6686b34eacf95a89e880b4a
Owner Address	0x36fed7c1c2199bd8a6686b34eacf95a89e880b4a

Audit Summary

Delivery Date	Oct 05, 2021
Audit Methodology	Static Analysis, Manual Review, Testnet Deployment
Key Components	Revolotto.sol

Vulnerability Summary

Vulnerability Level	Total
Critical	0
Major	1
Medium	0
Minor	1
Informational	1
Discussion	0

Understandings

The Revolotto Protocol is a decentralized finance (DeFi) token deployed on the Binance smart chain (BSC). Revolotto employs three novel features in its protocol; static rewards for each user, LP acquisition mechanism and Burn. The static reward (also known as reflection), Burn and LP acquisition mechanisms function as follows:

Each Revolotto transaction is taxed 20% fees of the transaction amount. The first 6% fee is redistributed to all existing holders using a form of rebasing mechanism whilst the other 9% is accumulated internally until a sufficient amount of capital has been amassed to perform an LP acquisition, and 5% Burns.

Introduction (Source: Whitepaper)

RVL is an abbreviation of RevoLotto. Collectively it is a four-dimensional Coin. On every trade 80% to the investor, 6% divided between all holders, 5% will be burnet, and 9% will automatically be added into Liquidity Pool and the coin will be locked into the locker contract which will be equal to the value of the coins, and its duration is three months. If any investor is holding it for three months not only, he will own multiple profits but also after the completion of the locker´s duration, he will be eligible for coins automatically as a bonus.

Apparently, every trade has a 20% fee but in reality, which is approximately about 5% because 5% Burn and 9% Locked coins are actually owned by the investor. But 5% burn, 9% adding into Liquidity pool and locking of Coin into Liquidity pool for three months is a hindrance to the investor to sell for a limited period of time. So as long as the price is up to the purchase price, many more investors will have come, which means that where the first investor will make a profit, many investors will have come, and the price will go up. No one will be able to pull down the price. And secondly, when there is 5% coins burn on each trade and 9% in the locker, the price will go up sharply, so who holds it longer, will be entitled to more profit.

Privileged Functions

The contract contains the following privileged functions that are restricted by the onlyOwner modifier. They are used to modify the contract configurations and address attributes. We grouped these functions below:

Account management functions for inclusion and exclusion in the fee:

excludeAccount(address account)

includeAccount(address account)

excludeAccountSender(address account)

includeAccountSender(address account)

Source Code (Verified)

Transactions | BEP-20 Token Txns | Contract | Events | Analytics | Comments

Code | Read Contract | Write Contract

Search Source Code

Contract Source Code Verified (Exact Match)

Contract Name:	**Revolotto**	Optimization Enabled:	**Yes** with **200** runs
Compiler Version	**v0.8.2+commit.661d1103**	Other Settings:	**default** evmVersion, **None** license

Contract Source Code (Solidity)

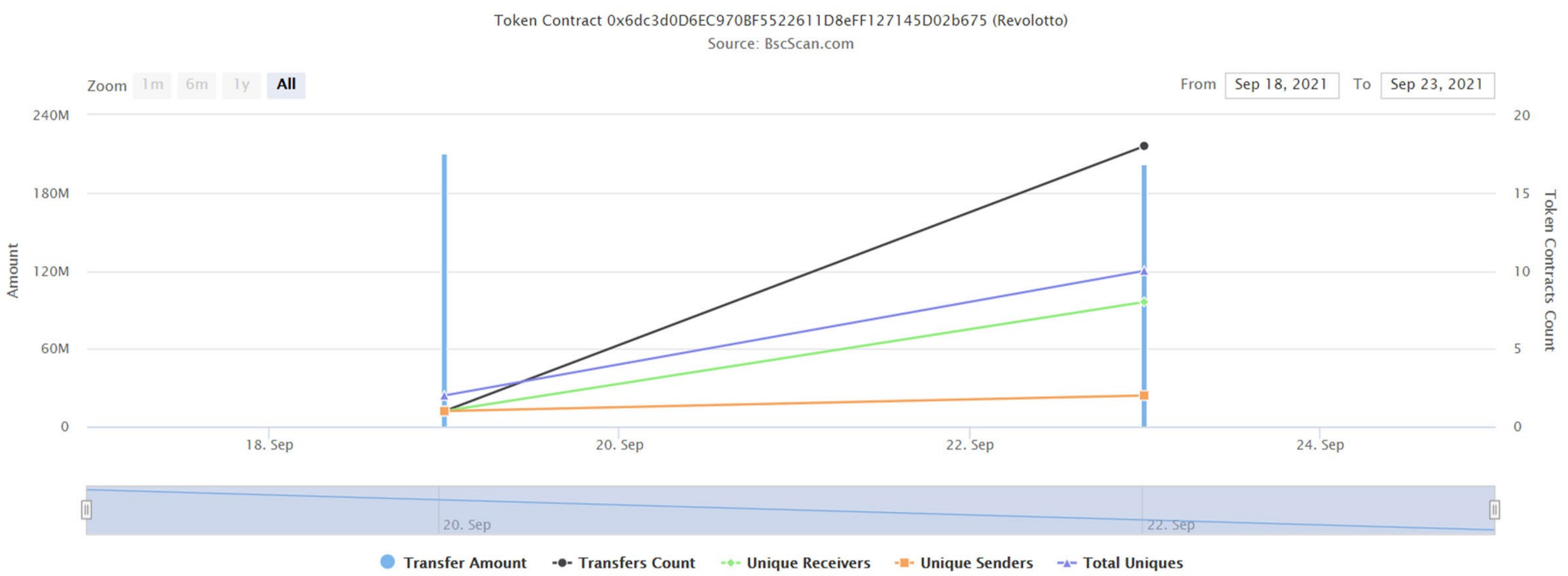
Outline | More Options

```
/**
 *Submitted for verification at BscScan.com on 2021-09-19
*/

// SPDX-License-Identifier: None

/**

 * Copyright © 2021 Revolotto - Revolutionary Lottery Coin. | All Rights Reserved
 * For more details please visit the website (www.revolotto.org)
 * contact: info@revolotto.org
 *
 * Revolotto is establishing the new standard of decentralized finance with its innovative coin circulation cycles and ultra burn system.
 * Holders are additionally "auto-staked" instantly receiving 6% of the transaction volume and they can watch their wallet grow in real-time.
 *
 * #Revolotto Contract Details & Features
 *
```

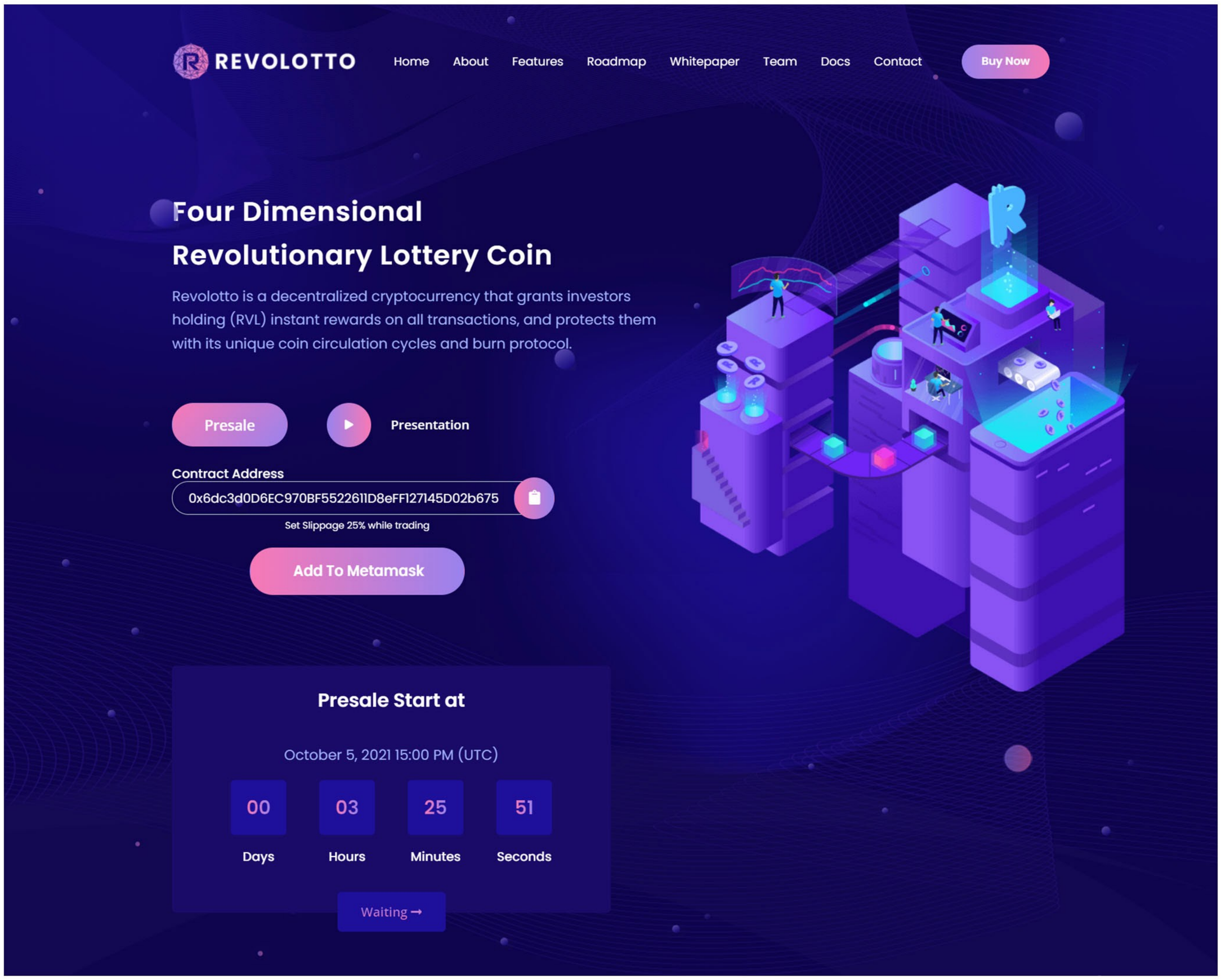
Contract Interaction

Time Series: Token Contract Overview

Sun 19, Sept 2021 - Thu 23, Sept 2021



Website Test (SSL Secured) www.revolotto.org



Latest Performance Report for:

https://revolotto.org/

Report generated: Mon, Oct 2, 2021 11:58 PM -0700
Test Server Location: Vancouver, Canada
Using: Chrome (Desktop) 90.0.4430.212, Lighthouse 8.3.0

GTmetrix Grade ?

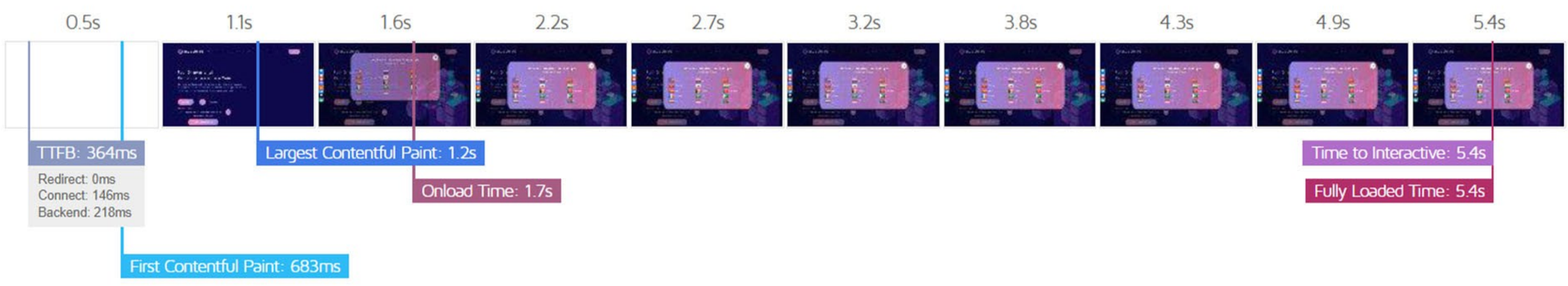
	Performance ?	Structure ?
B	78%	88%

Web Vitals ?

LCP ?	TBT ?	CLS ?
1.2s	277ms	0

Summary | Performance | Structure | Waterfall | Video | History

Speed Visualization ?



Contract Function Details

Int IBEP20
[Ext] totalSupply
[Ext] balanceOf
[Ext] transfer #
[Ext] allowance
[Ext] approve #
[Ext] transferFrom #

[Lib] SafeMath
[Int] add
[Int] sub
[Int] mul
[Int] div
[Int] mod

Context
[Int] _msgSender

[Lib] Address
[Int] isContract
[Int] sendValue #
[Int] functionCall #
[Int] functionCall #
[Int] functionCallWithValue #
[Int] functionCallWithValue #

Revolotto (Context, IBEP20, Ownable)
[Pub] (String) Website = "www.revolotto.org"

[Pub] <constructor>
[Pub] name
[Pub] symbol
[Pub] decimals
[Pub] totalSupply
[Pub] balanceOf
[Pub] transfer #
[Pub] allowance
[Pub] approve #
[Pub] transferFrom #
[Pub] increaseAllowance #
[Pub] decreaseAllowance #
[Pub] isExcluded
[Pub] isExcludedSender

[Pub] totalFees
[Pub] totalBurn
[Pub] totalLiquidityPool
[Pub] deliver #
[Pub] reflectionFromToken
[Pub] tokenFromReflection

[Ext] excludeAccount #
- modifiers: onlyOwner()

[Ext] includeAccount #
- modifiers: onlyOwner()

[Ext] excludeAccountSender #
- modifiers: onlyOwner()

[Ext] includeAccountSender #
- modifiers: onlyOwner()

[Ext] setAsLiquidityPoolAccount #
- modifiers: onlyOwner()

[Ext] updateFee #
- modifiers: onlyOwner()

[Prv] _approve
[Prv] _transfer
[Prv] _transferStandard
[Prv] _standardTransferContent
[Prv] _transferToExcluded
[Prv] _excludedFromTransferContent
[Prv] _transferFromExcluded
[Prv] _excludedToTransferContent
[Prv] _transferBothExcluded
[Prv] _bothTransferContent
[Prv] _reflectFee
[Prv] _getValues
[Prv] _getTBasics
[Prv] getTTransferAmount
[Prv] _getRBasics
[Prv] _getRTransferAmount
[Prv] _getRate
[Prv] _getCurrentSupply

[Prv] _sendToLiquidityPool
[Prv] removeAllFee
[Prv] restoreAllFee
[Ext] withdraw

Issues Checking System

Issue Description	Checking Status
Compiler errors	Passed
Race conditions and Reentrancy	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Timestamp dependence	Passed
Integer Overflow and Underflow	Passed
DoS with Revert	Passed
DoS with block gas limit	Low Issues
Methods execution permissions	Passed
Economy model of the contract	Passed
The impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and Declaration	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Design Logic	Passed

Security Issues

High Severity Issues

No high severity issues were found.

Medium Severity Issues

No medium severity issues were found.

Low Severity Issues

1. Out of gas

Issue:

- **The function includeAccount() uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.**

```
function includeAccount(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already included");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- **The function _getCurrentSupply also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.**

```
function _getCurrentSupply() private view returns(uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] >
        tSupply) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big

Owner privileges (In the period when the owner is not renounced)

- **Owner can change the tax, liquidity, burn fee.**

```
function updateFee(uint256 _txFee,uint256 _burnFee,uint256
_liquiditypoolFee) onlyOwner() public{
    require(_txFee < 100 && _burnFee < 100 && _liquiditypoolFee < 100);
    _TAX_FEE = _txFee* 100;
     BURN_FEE =  burnFee * 100;
    _LIQUIDITYPOOL_FEE = _liquiditypoolFee* 100;
    ORIG_TAX_FEE = _TAX_FEE;
    ORIG_BURN_FEE = _BURN_FEE;
    ORIG_LIQUIDITYPOOL_FEE = _LIQUIDITYPOOL_FEE;
}
```

- **Owner can exclude from the fee.**

```
function excludeAccount(address account) external onlyOwner() {
    require(!_isExcluded[account], "Account is already excluded");
    if(_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}
```

Conclusion

- Smart contracts contain low severity issues!

Liquidity Locking Details:

- Liquidity will be locked on Digital Ocean Locker (5 Years) after pancake listing

In contract Revolotto, there are bunch of functions can change state variables. However these function do not emit event to pass the changes out of chain.

Recommendation

Recommend emitting events, for all the essential state variables that are possible to be changed during runtime.

Digital Ocean Note:

Please check the disclaimer above and note. The report is provided for the only contract mentioned in the report and does not include any other potentioal contracts deployed by Owner.

Disclaimer

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Digital Ocean and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (Digital Ocean) owe no duty of care towards you or any other person, nor does Digital Ocean make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties, or other terms of any kind except as set out in this disclaimer, and Digital Ocean hereby excludes all representations, warranties, conditions, and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Digital Ocean hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Digital Ocean, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent), or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use, or the results of the use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

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 Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with 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, nor may copies be delivered to any other person other than the Company, without Digital Ocean’s prior written consent in each instance.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Digital Ocean to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide an indication of the technologies proprietors, business, business model, or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Digital Ocean’s position is that each company and individual are responsible for their own due diligence and continuous security.

Digital Ocean’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or the functionality of the technology we agree to analyze.

The assessment services provided by Digital Ocean are subject to dependencies and are under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND “AS Revolotto Security Assessment AVAILABLE” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, Digital Ocean HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORTS, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, Digital Ocean SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, Digital Ocean MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER’S OR ANY OTHER PERSON’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, Digital Ocean PROVIDES NO WARRANTY OR UNDERTAKING AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR-FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER Digital Ocean NOR ANY OF DIGITAL OCEAN’S AGENTS MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. Digital Ocean WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER’S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED “AS IS” AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN THE CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT Digital Ocean’S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF SHALL BE A THIRD PARTY OR OTHER BENEFICIARIES OF SUCH SERVICES, ASSESSMENT REPORTS, AND ANY ACCOMPANYING Revolotto Security Assessment MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST DIGITAL OCEAN WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORTS, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF THE DIGITAL OCEAN CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMERS. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST DIGITAL OCEAN WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OF ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

DIGITAL OCEAN

Security Assessment

Revolotto

Oct 5th, 2021

digitalocean.finance