



Oropay

# Smart Contract Audit Report

# TABLE OF CONTENTS

## Audited Details

- Audited Project
- Blockchain
- Addresses
- Project Website
- Codebase

## Summary

- Contract Summary
- Audit Findings Summary
- Vulnerabilities Summary

## Conclusion

## Audit Results

## Smart Contract Analysis

- Detected Vulnerabilities

## Disclaimer

## About Us

# AUDITED DETAILS

## Audited Project

Project name	Token ticker	Blockchain
Oropay	OPAY	Binance Smart Chain

## Addresses

Contract address	0xe8ad9d938a4ab6cea6aae0ae3ae07b546069e2aa
Contract deployer address	0x68fA3a654684f22809d3E5959dECC26b0ea8d3dc

## Project Website

<https://www.oropay.io/>

## Codebase

<https://bscscan.com/address/0xe8ad9d938a4ab6cea6aae0ae3ae07b546069e2aa#code>

# SUMMARY

Oropay token creates a community to grow an economy via the BSC blockchain. Oropay Pass looks to connect the world through cryptocurrencies. With our strong development team, we have created an interface to bring the NFT market to your hands quickly. Join our community today to help us develop Oropay Token.

## Contract Summary

### Documentation Quality

Oropay provides a very poor documentation with standard of solidity base code.

- The technical description is provided unclear and disorganized.

### Code Quality

The Overall quality of the basecode is poor.

- Solidity basecode and rules are unclear and disorganized by Oropay.

### Test Coverage

Test coverage of the project is 100% ( Through Codebase )

## Audit Findings Summary

- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 178.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 20.

## CONCLUSION

We have audited the Oropay project released on October 2021 to find issues and identify potential security vulnerabilities in the Oropay project. This process is used to find technical issues and security loopholes that may be found in smart contracts.

The security audit report yielded unsatisfactory results, discovering high-risk and low-risk issues.

Writing a contract that does not follow the Solidity style guide can pose a significant risk. The serious and low problems we found in the smart contract are The arithmetic operator can overflow, and It is possible to cause an integer overflow or underflow in the arithmetic operation. Low-risk found is a floating pragma is set; the current pragma Solidity directive is "`^0.6.12`". Specifying a fixed compiler version is recommended to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

We were recommended to keep being aware of investing in this risky smart contract.

# AUDIT RESULT

Article	Category	Description	Result
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	PASS
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	ISSUE FOUND
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	PASS
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	ISSUE FOUND
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	PASS
Unprotected Ether Withdrawal	SWC-105	Due to missing or insufficient access controls, malicious parties can withdraw from the contract.	PASS
SELFDESTRUCT Instruction	SWC-106	The contract should not be self-destructible while it has funds belonging to users.	PASS
Reentrancy	SWC-107	Check effect interaction pattern should be followed if the code performs recursive call.	PASS
Uninitialized Storage Pointer	SWC-109	Uninitialized local storage variables can point to unexpected storage locations in the contract.	PASS
Assert Violation	SWC-110 SWC-123	Properly functioning code should never reach a failing assert statement.	PASS
Deprecated Solidity Functions	SWC-111	Deprecated built-in functions should never be used.	PASS
Delegate call to Untrusted Callee	SWC-112	Delegatecalls should only be allowed to trusted addresses.	PASS

DoS (Denial of Service)	SWC-113 SWC-128	Execution of the code should never be blocked by a specific contract state unless required.	PASS
Race Conditions	SWC-114	Race Conditions and Transactions Order Dependency should not be possible.	PASS
Authorization through tx.origin	SWC-115	tx.origin should not be used for authorization.	PASS
Block values as a proxy for time	SWC-116	Block numbers should not be used for time calculations.	PASS
Signature Unique ID	SWC-117 SWC-121 SWC-122	Signed messages should always have a unique id. A transaction hash should not be used as a unique id.	PASS
Incorrect Constructor Name	SWC-118	Constructors are special functions that are called only once during the contract creation.	PASS
Shadowing State Variable	SWC-119	State variables should not be shadowed.	PASS
Weak Sources of Randomness	SWC-120	Random values should never be generated from Chain Attributes or be predictable.	PASS
Write to Arbitrary Storage Location	SWC-124	The contract is responsible for ensuring that only authorized user or contract accounts may write to sensitive storage locations.	PASS
Incorrect Inheritance Order	SWC-125	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order. The rule of thumb is to inherit contracts from more /general/ to more /specific/.	PASS
Insufficient Gas Griefing	SWC-126	Insufficient gas griefing attacks can be performed on contracts which accept data and use it in a sub-call on another contract.	PASS
Arbitrary Jump Function	SWC-127	As Solidity doesnt support pointer arithmetics, it is impossible to change such variable to an arbitrary value.	PASS

<b>Typographical Error</b>	<b>SWC-129</b>	A typographical error can occur for example when the intent of a defined operation is to sum a number to a variable.	<b>PASS</b>
<b>Override control character</b>	<b>SWC-130</b>	Malicious actors can use the Right-To-Left-Override unicode character to force RTL text rendering and confuse users as to the real intent of a contract.	<b>PASS</b>
<b>Unused variables</b>	<b>SWC-131 SWC-135</b>	Unused variables are allowed in Solidity and they do not pose a direct security issue.	<b>PASS</b>
<b>Unexpected Ether balance</b>	<b>SWC-132</b>	Contracts can behave erroneously when they strictly assume a specific Ether balance.	<b>PASS</b>
<b>Hash Collisions Variable</b>	<b>SWC-133</b>	Using <code>abi.encodePacked()</code> with multiple variable length arguments can, in certain situations, lead to a hash collision.	<b>PASS</b>
<b>Hardcoded gas amount</b>	<b>SWC-134</b>	The <code>transfer()</code> and <code>send()</code> functions forward a fixed amount of 2300 gas.	<b>PASS</b>
<b>Unencrypted Private Data</b>	<b>SWC-136</b>	It is a common misconception that private type variables cannot be read.	<b>PASS</b>



# SMART CONTRACT ANALYSIS

Started	Wednesday Oct 27 2021 21:52:34 GMT+0000 (Coordinated Universal Time)
Finished	Thursday Oct 28 2021 19:31:20 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	Oropay.sol

## Detected Issues

ID	Title	Severity	Status
SWC-101	THE ARITHMETIC OPERATOR CAN OVERFLOW.	high	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged

# SWC-101 | THE ARITHMETIC OPERATOR CAN OVERFLOW.

LINE 178

## high SEVERITY

It is possible to cause an integer overflow or underflow in the arithmetic operation.

## Source File

- Oropay.sol

## Locations

```
177  _owner = address(0);
178  _lockTime = now + time;
179  emit OwnershipTransferred(_owner, address(0));
180  }
181
182
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 20

### low SEVERITY

The current pragma Solidity directive is `^0.6.12`. It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

### Source File

- Oropay.sol

### Locations

```
19 // SPDX-License-Identifier: MIT
20 pragma solidity ^0.6.12;
21
22 abstract contract Context {
23     function _msgSender() internal view virtual returns (address payable) {
24
```

# DISCLAIMER

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 Sysfixed’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 Sysfixed 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 any indication of the technologies proprietors, business, business model, or legal compliance.

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 below disclaimer below – please make sure to read it in full.

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.

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 Sysfixed and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (Sysfixed) owe no duty of care.

## ABOUT US

Sysfixed is a blockchain security certification organization established in 2021 with the objective to provide smart contract security services and verify their correctness in blockchain-based protocols. Sysfixed automatically scans for security vulnerabilities in Ethereum and other EVM-based blockchain smart contracts. Sysfixed a comprehensive range of analysis techniques—including static analysis, dynamic analysis, and symbolic execution—can accurately detect security vulnerabilities to provide an in-depth analysis report. With a vibrant ecosystem of world-class integration partners that amplify developer productivity, Sysfixed can be utilized in all phases of your project's lifecycle. Our team of security experts is dedicated to the research and improvement of our tools and techniques used to fortify your code.