December 14, 2023

Express Audit Report for

Biopay Token [BPYT]

De.Fi

De.Fi

Project Summary

Project Name	BiopayToken(Biopay Token)
Address	0x89b43692c680481a3d406c4c8701c93784b14989
Network	56

De.Fi

Issue ID	107
Severity	Low
Status	Medium

Description Code	**function approveAndCall**(**address** spender, **uint** tokens, **bytes** data) **public returns** (**bool** success) {
	allowed[msg.sender][spender] = tokens;
	emit Approval(msg.sender, spender, tokens);
	ApproveAndCallFallBack(spender).receiveApproval(
	msg.sender, tokens, this, data);
	return true;
	}

Location	Reentrancy in BiopayToken.approveAndCall(address,uint256,bytes) (BiopayToken.sol#202-207): - in expression:ApproveAndCallFallBack(spender).receiveApproval(msg.sender,tokens,this,data)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function totalSupply**() **public constant returns** (**uint**) {
	return _totalSupply - balances[**address**(0)];
	}

Location	totalSupply() should be declared external: - BiopayToken.totalSupply() (BiopayToken.sol#129-131) - ERC20Interface.totalSupply() (BiopayToken.sol#47)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function balanceOf**(**address** tokenOwner) **public constant returns** (**uint** balance) {
	return balances[tokenOwner];
	}

Location	balanceOf(address) should be declared external: - BiopayToken.balanceOf(address) (BiopayToken.sol#137-139) - ERC20Interface.balanceOf(address) (BiopayToken.sol#48)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function transfer**(**address** to, **uint** tokens) **public returns** (**bool** success) {
	balances[msg.sender] =
	safeSub(balances[msg.sender], tokens);
	balances[to] = safeAdd(balances[to], tokens);
	emit Transfer(msg.sender, to, tokens);
	return true;
	}

Location	transfer(address,uint256) should be declared external: - BiopayToken.transfer(address,uint256) (BiopayToken.sol#147-152) - ERC20Interface.transfer(address,uint256) (BiopayToken.sol#50)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function approve**(**address** spender, **uint** tokens)
	public returns (**bool** success) {
	allowed[msg.sender][spender] = tokens;
	emit Approval(msg.sender, spender, tokens);
	return true;
	}

Location	approve(address,uint256) should be declared external: - BiopayToken.approve(address,uint256) (BiopayToken.sol#163-167) - ERC20Interface.approve(address,uint256) (BiopayToken.sol#51)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function transferFrom**(**address from**, **address** to, **uint** tokens) **public returns** (**bool** success) {
	balances[**from**] = safeSub(balances[**from**], tokens);
	allowed[**from**][msg.sender] = safeSub(allowed[**from**][msg.sender], tokens);
	balances[to] = safeAdd(balances[to], tokens);
	emit Transfer(**from**, to, tokens);
	return true;
	}

Location	transferFrom(address,address,uint256) should be declared external: - BiopayToken.transferFrom(address,address,uint256) (BiopayToken.sol#179-185) - ERC20Interface.transferFrom(address,address,uint256) (BiopayToken.sol#52)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function allowance**(**address** tokenOwner, **address** spender) **public constant returns** (**uint** remaining)
	{
	return allowed[tokenOwner][spender];
	}

Location	allowance(address,address) should be declared external: - BiopayToken.allowance(address,address) (BiopayToken.sol#192-194) - ERC20Interface.allowance(address,address) (BiopayToken.sol#49)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function approveAndCall**(**address** spender, **uint** tokens, **bytes** data) **public returns** (**bool** success) {
	allowed[msg.sender][spender] = tokens;
	emit Approval(msg.sender, spender, tokens);
	ApproveAndCallFallBack(spender).receiveApproval(
	msg.sender, tokens, this, data);
	return true;
	}

Location	approveAndCall(address,uint256,bytes) should be declared external: - BiopayToken.approveAndCall(address,uint256,bytes) (BiopayToken.sol#202-207)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function** () **public payable** {
	revert();
	}

Location	fallback() should be declared external: - BiopayToken.fallback() (BiopayToken.sol#213-215)

De.Fi

Issue ID	184
Severity	Optimization
Status	High

Description Code	**function transferAnyERC20Token**(**address** tokenAddress, **uint** tokens) **public onlyOwner returns** (**bool** success) {
	return ERC20Interface(tokenAddress).transfer(owner, tokens);
	}

Location	transferAnyERC20Token(address,uint256) should be declared external: - BiopayToken.transferAnyERC20Token(address,uint256) (BiopayToken.sol#221-223)

De.Fi

Issue ID	177
Severity	Informational
Status	High
Description Code	**pragma solidity** ^0.4.24;
Location	Pragma version^0.4.24 (BiopayToken.sol#2) allows old versions

De.Fi

Issue ID	177
Severity	Informational
Status	High
Description Code	
Location	solc-0.4.24 is not recommended for deployment

De.Fi

Issue ID	168
Severity	Low
Status	Medium
Description Code	**function transferOwnership**(**address** _newOwner) **public onlyOwner** {
Location	Owned.transferOwnership(address)._newOwner (BiopayToken.sol#87) lacks a zero-check on : - newOwner = _newOwner (BiopayToken.sol#88)

De.Fi

Issue ID	182
Severity	Informational
Status	Medium

Description Code	**constructor**() **public** {
	symbol = "BPYT";
	name = "Biopay Token";
	decimals = 18;
	_totalSupply = 100000000000000000000000000;
	balances[0x2F8215cd83292A2230f4a712644E4de9258b735d] = _totalSupply;
	emit Transfer(**address**(0), 0x2F8215cd83292A2230f4a712644E4de9258b735d, _totalSupply);
	}

Location	BiopayToken.constructor() (BiopayToken.sol#116-123) uses literals with too many digits: - _totalSupply = 100000000000000000000000000 (BiopayToken.sol#120)