



October 21, 2023

Audit Report for


QuantumUnit





Project Summary


Project Name	QuantumUnit
Address	0x958c860c0195c0f66fbe46e3bad2f416964c25e8
Network	56


Detectors


 No vulnerable withdrawal functions found


 No locks detected


 Verified source code found


 No ERC20 approval vulnerability found


 Contract owner cannot abuse ERC20 approvals

 No blocking loops found

 Wallets cannot be blacklisted from any specific contract functionality

 No functionality can be paused by the contract owner

 No approval restrictions found

 No vulnerable ownership functions found.



De.Fi



No retrievable ownership found.



No mixers utilized by contract deployer.



No previous scams by owner's wallet found.



Recent Interaction was within 30 Days.

Interaction with the smart contract was less than 30 days ago



Initializer is Protected from re-execution.

General Detectors



Floating Pragma

This contract may not function as expected due to inconsistent solidity compiler versions being specified.



Division Before Multiplication

The order of operations used may result in a loss of precision.



Uninitialized Local Variables

This contract's local variables are not all initialized, potentially resulting in lost funds or other exploits.



Missing Arithmetic Events

This contract is missing useful arithmetic events.



Missing Zero Address Validation

Some functions in this contract may not appropriately check for zero addresses being used.



Low Level Calls

This contract uses low level calls, which may be unsafe.



Incorrect Solidity Version

This contract uses an unconventional or very old version of Solidity.



Numeric Notation Best Practices

The numeric notation used in this contract is unconventional, possibly worsening the reading/debugging experience.



Public Functions Should be Declared External

Some functions in this contract should be declared as external in order to save gas.



De.Fi

- ✓ No unchecked call responses found

- ✓ No vulnerable self-destruct functions found

- ✓ No assertion vulnerabilities found

- ✓ No old solidity code found

- ✓ No external delegated calls found

- ✓ No external call dependency found

- ✓ No vulnerable authentication calls found

- ✓ No invalid character typos found

- ✓ No RTL characters found

- ✓ No dead code found



De.Fi

- ✓ No risky data allocation found
- ✓ No uninitialized state variables found
- ✓ No uninitialized storage variables found
- ✓ No vulnerable initialization functions found
- ✓ No risky data handling found
- ✓ No number accuracy bug found
- ✓ No out-of-range number vulnerability found
- ✓ No map data deletion vulnerabilities found
- ✓ No tautologies or contradictions found
- ✓ No faulty true/false values found



De.Fi

✓ No redundant constructor calls found

✓ No vulnerable transfers found

✓ No vulnerable return values found

✓ No default function responses found

✓ No missing access control events found

✓ No redundant true/false comparisons found


✓ No state variables vulnerable through function calls found


✓ No expensive loops found

✓ No missing constant declarations found


✓ No vulnerable payable functions found

✓ No vulnerable message values found

Issue ID	103
Severity	 High
Status	Informational
Description Code	<code>pragma solidity ^0.8.0;</code>
Location	<p>Different versions of Solidity is used:</p> <ul style="list-style-type: none">- Version used: ['^0.8.0', '^0.8.1', '^0.8.18', '^0.8.2']- ^0.8.0 (QuantumUnit.sol#21)- ^0.8.0 (QuantumUnit.sol#161)- ^0.8.0 (QuantumUnit.sol#190)- ^0.8.0 (QuantumUnit.sol#209)- ^0.8.1 (QuantumUnit.sol#232)- ^0.8.2 (QuantumUnit.sol#479)- ^0.8.2 (QuantumUnit.sol#647)- ^0.8.0 (QuantumUnit.sol#819)- ^0.8.0 (QuantumUnit.sol#933)- ^0.8.0 (QuantumUnit.sol#973)- ^0.8.18 (QuantumUnit.sol#1069)- ^0.8.0 (QuantumUnit.sol#1101)- ^0.8.18 (QuantumUnit.sol#1861)

Issue ID	184
Severity	 High
Status	Optimization
Description Code	<pre>function initialize(address _tokenAddress) initializer public { __Ownable_init(); __UUPSUpgradeable_init(); protocolFeePercent = 5000000000000000; refererFeePercent = 5000000000000000; withdrawFee = 10000000000000000; minInvestSum = 10000000000000000; minWithdrawSum = 5000000000000000; tokenReward = 5000000000000000; interestPerBlock = 347222222200; blockEverySecond = 3; tokenAddress = _tokenAddress; tokenContract = IERC20(tokenAddress); }</pre>
Location	<p>initialize(address) should be declared external:</p> <ul style="list-style-type: none">- QuantumUnit.initialize(address) <p>(QuantumUnit.sol#1874-1888)</p>


Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<pre> function invest(address referer) public payable { require(msg.value >= minInvestSum, "Your investment amount must be greater"); users[msg.sender] = getBalance(msg.sender) + msg.value; totalInvested += msg.value; if (lastInvest[msg.sender] == 0) { totalUsers++; } lastInvest[msg.sender] = block.timestamp; uint256 protocolFee = msg.value * protocolFeePercent / 1 ether; uint256 refererFee = msg.value * refererFeePercent / 1 ether; (bool success1,) = owner().call{value: protocolFee} (""); (bool success2,) = referer.call{value: refererFee}(""); totalReferralPaided += refererFee; require(success1 && success2, "Unable to invest"); emit Invest(msg.sender, referer, msg.value); } </pre>
Location	invest(address) should be declared external: - QuantumUnit.invest(address) (QuantumUnit.sol#1919-1938)


Issue ID	184
Severity	 High
Status	Optimization
Description Code	function withdrawAll() public { withdraw(getBalance(msg.sender)); }
Location	withdrawAll() should be declared external: - QuantumUnit.withdrawAll() (QuantumUnit.sol#1956-1958)

Issue ID	184
Severity	🎯 High
Status	Optimization
Description Code	function setProtocolFeePercent(uint256 _feePercent) public onlyOwner { protocolFeePercent = _feePercent; }
Location	setProtocolFeePercent(uint256) should be declared external: - QuantumUnit.setProtocolFeePercent(uint256) (QuantumUnit.sol#1984-1986)

Issue ID	184
Severity	 High
Status	Optimization
Description Code	function setRefererFeePercent(uint256 _feePercent) public onlyOwner { refererFeePercent = _feePercent; }
Location	setRefererFeePercent(uint256) should be declared external: - QuantumUnit.setRefererFeePercent(uint256) (QuantumUnit.sol#1988-1990)


Issue ID	184
Severity	 High
Status	Optimization
Description Code	function setMinInvestSum(uint256 _sum) public onlyOwner { minInvestSum = _sum; }
Location	setMinInvestSum(uint256) should be declared external: - QuantumUnit.setMinInvestSum(uint256) (QuantumUnit.sol#1992-1994)


Issue ID	184
Severity	 High
Status	Optimization
Description Code	function setMinWithdrawSum(uint256 _sum) public onlyOwner { minWithdrawSum = _sum; }
Location	setMinWithdrawSum(uint256) should be declared external: - QuantumUnit.setMinWithdrawSum(uint256) (QuantumUnit.sol#1996-1998)


Issue ID	184
Severity	 High
Status	Optimization
Description Code	function setWithdrawFee(uint256 _feePercent) public onlyOwner { withdrawFee = _feePercent; }
Location	setWithdrawFee(uint256) should be declared external: - QuantumUnit.setWithdrawFee(uint256) (QuantumUnit.sol#2000-2002)

Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	function setInterestPerBlock(uint256 _interest) public onlyOwner { interestPerBlock = _interest; }
Location	setInterestPerBlock(uint256) should be declared external: - QuantumUnit.setInterestPerBlock(uint256) (QuantumUnit.sol#2004-2006)

Issue ID	184
Severity	🎯 High
Status	Optimization
Description Code	<pre>function setBlockEverySecond(uint256 _blocks) public onlyOwner { blockEverySecond = _blocks; }</pre>
Location	<p>setBlockEverySecond(uint256) should be declared external:</p> <ul style="list-style-type: none">- QuantumUnit.setBlockEverySecond(uint256) (QuantumUnit.sol#2008-2010)


Issue ID	184
Severity	 High
Status	Optimization
Description Code	<pre>function setTokenAddress(address _address) public onlyOwner { tokenAddress = _address; tokenContract = IERC20(tokenAddress); }</pre>
Location	<p>setTokenAddress(address) should be declared external:</p> <ul style="list-style-type: none">- QuantumUnit.setTokenAddress(address) <p>(QuantumUnit.sol#2012-2015)</p>


Issue ID	184
Severity	 High
Status	Optimization
Description Code	<pre>function setTokenReward(uint256 _tokenReward) public onlyOwner { tokenReward = _tokenReward; }</pre>
Location	<p>setTokenReward(uint256) should be declared external:</p> <ul style="list-style-type: none">- QuantumUnit.setTokenReward(uint256) <p>(QuantumUnit.sol#2017-2019)</p>

Issue ID	177
Severity	 High
Status	Informational
Description Code	<code>pragma solidity ^0.8.0;</code>
Location	Pragma version^0.8.0 (QuantumUnit.sol#21) allows old versions



De.Fi

Issue ID	177
Severity	 High
Status	Informational
Description Code	<code>pragma solidity ^0.8.1;</code>
Location	Pragma version^0.8.1 (QuantumUnit.sol#232) allows old versions

Issue ID	177
Severity	 High
Status	Informational
Description Code	<code>pragma solidity ^0.8.2;</code>
Location	Pragma version^0.8.2 (QuantumUnit.sol#479) allows old versions



De.Fi

Issue ID	177
Severity	🎯 High
Status	Informational
Description Code	<code>pragma solidity ^0.8.18;</code>
Location	Pragma version^0.8.18 (QuantumUnit.sol#1069) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7



De.Fi

Issue ID	177
Severity	🎯 High
Status	Informational
Description Code	
Location	solc-0.8.18 is not recommended for deployment

Issue ID	173
Severity	🔴 High
Status	Informational
Description Code	<pre> function invest(address referer) public payable { require(msg.value >= minInvestSum, "Your investment amount must be greater"); users[msg.sender] = getBalance(msg.sender) + msg.value; totalInvested += msg.value; if (lastInvest[msg.sender] == 0) { totalUsers++; } lastInvest[msg.sender] = block.timestamp; uint256 protocolFee = msg.value * protocolFeePercent / 1 ether; uint256 refererFee = msg.value * refererFeePercent / 1 ether; (bool success1,) = owner().call{value: protocolFee} (""); (bool success2,) = referer.call{value: refererFee}(""); totalReferralPaided += refererFee; require(success1 && success2, "Unable to invest"); emit Invest(msg.sender, referer, msg.value); } </pre>
Location	<p>Low level call in QuantumUnit.invest(address) (QuantumUnit.sol#1919-1938):</p> <ul style="list-style-type: none"> - (success1) = owner().call{value: protocolFee}() (QuantumUnit.sol#1932) - (success2) = referer.call{value: refererFee}() (QuantumUnit.sol#1933)

Issue ID	173
Severity	🔴 High
Status	Informational
Description Code	<pre> function withdraw(uint256 sum) public { uint256 balance = getBalance(msg.sender); require(balance >= sum, "You do not have enough funds to withdraw"); require(sum >= minWithdrawSum, "Withdrawal amount below minimum"); totalWithdrawn += sum; users[msg.sender] = balance - sum; lastInvest[msg.sender] = block.timestamp; uint256 withdrawSum = sum - sum * withdrawFee / 1 ether; (bool success1,) = msg.sender.call{ value: withdrawSum }(""); require(success1, "Unable to withdraw"); tokenContract.mint(msg.sender, sum * tokenReward / 1 ether); emit Withdraw(msg.sender, sum); } </pre>
Location	<p>Low level call in QuantumUnit.withdraw(uint256) (QuantumUnit.sol#1940-1954):</p> <p>- (success1) = msg.sender.call{value: withdrawSum}() (QuantumUnit.sol#1949)</p>

Issue ID	167-a
Severity	🎯 Medium
Status	Low
Description Code	function setInterestPerBlock(uint256 _interest) public onlyOwner { interestPerBlock = _interest; }
Location	QuantumUnit.setInterestPerBlock(uint256) (QuantumUnit.sol#2004-2006) should emit an event for: - interestPerBlock = _interest (QuantumUnit.sol#2005)

Issue ID	167-a
Severity	🔴 Medium
Status	Low
Description Code	function setBlockEverySecond(uint256 _blocks) public onlyOwner { blockEverySecond = _blocks; }
Location	QuantumUnit.setBlockEverySecond(uint256) (QuantumUnit.sol#2008-2010) should emit an event for: - blockEverySecond = _blocks (QuantumUnit.sol#2009)

Issue ID	168
Severity	🟠 Medium
Status	Low
Description Code	function initialize(address _tokenAddress) initializer public {
Location	QuantumUnit.initialize(address)._tokenAddress (QuantumUnit.sol#1874) lacks a zero-check on : - tokenAddress = _tokenAddress (QuantumUnit.sol#1886)



Issue ID	168
Severity	🎯 Medium
Status	Low
Description Code	function invest(address referer) public payable {
Location	QuantumUnit.invest(address).referer (QuantumUnit.sol#1919) lacks a zero-check on : - (success2) = referer.call{value: refererFee}() (QuantumUnit.sol#1933)

Issue ID	168
Severity	🔴 Medium
Status	Low
Description Code	function setTokenAddress(address _address) public onlyOwner {
Location	QuantumUnit.setTokenAddress(address)._address (QuantumUnit.sol#2012) lacks a zero-check on : - tokenAddress = _address (QuantumUnit.sol#2013)

Issue ID	107
Severity	🟡 Medium
Status	High
Description Code	<pre> function invest(address referer) public payable { require(msg.value >= minInvestSum, "Your investment amount must be greater"); users[msg.sender] = getBalance(msg.sender) + msg.value; totalInvested += msg.value; if (lastInvest[msg.sender] == 0) { totalUsers++; } lastInvest[msg.sender] = block.timestamp; uint256 protocolFee = msg.value * protocolFeePercent / 1 ether; uint256 refererFee = msg.value * refererFeePercent / 1 ether; (bool success1,) = owner().call{value: protocolFee} (""); (bool success2,) = referer.call{value: refererFee}(""); totalReferralPaided += refererFee; require(success1 && success2, "Unable to invest"); emit Invest(msg.sender, referer, msg.value); } </pre>
Location	<p>Reentrancy in QuantumUnit.invest(address) (QuantumUnit.sol#1919-1938): External calls sending eth: - (success2) = referer.call{value: refererFee}()</p> <p>State variables written after the call(s): - totalReferralPaided += refererFee</p>

Issue ID	182
Severity	🔴 Medium
Status	Informational
Description Code	<pre>function initialize(address _tokenAddress) initializer public { __Ownable_init(); __UUPSUpgradeable_init(); protocolFeePercent = 5000000000000000; refererFeePercent = 5000000000000000; withdrawFee = 10000000000000000; minInvestSum = 10000000000000000; minWithdrawSum = 5000000000000000; tokenReward = 5000000000000000; interestPerBlock = 347222222200; blockEverySecond = 3; tokenAddress = _tokenAddress; tokenContract = IERC20(tokenAddress); }</pre>
Location	<p>QuantumUnit.initialize(address) (QuantumUnit.sol#1874-1888) uses literals with too many digits:</p> <ul style="list-style-type: none">- protocolFeePercent = 5000000000000000 (QuantumUnit.sol#1877)

Issue ID	182
Severity	🎯 Medium
Status	Informational
Description Code	uint256 public protocolFeePercent = 50000000000000000;
Location	Contract QuantumUnit uses literals with too many digits: - protocolFeePercent = 50000000000000000 (QuantumUnit.sol#1896)