MultiSig Audit Report

On testing all the contract functions behave as they are intended to be. Unit tests that checked various behavior scenarios worked as intended

- Requirements: MultiSig requirements
- Code
- Version: 1.0
- Test Cases

Audit Report

Function & State Variable Default Visibility

NO risk and vulnerabilities as all the variables are defined with visibility explicitly.

Integer Overflow and Underflow

NO risk and vulnerabilities

Unchecked Call Return Value

NO risk and vulnerabilities as there are no low level calls included in the contract

Unprotected Ether Withdrawal

NO risk and vulnerabilities

Unprotected Self Destruct Instruction

NO risk and vulnerabilities

REENTRANCY ATTACK

NO risk and vulnerabilities.No external contracts are being called

Uninitialized Storage Pointer

NO risk and vulnerabilities

Assert Violation

NO risk and vulnerabilities.No assert functions are used

Use of Deprecated Solidity Functions

NO risk and vulnerabilities.No deprecated solidity functions are used

Delegatecall to Untrusted Callee

NO risk and vulnerabilities

DoS with Failed Call

NO risk and vulnerabilities. No external calls made on the contract

Transaction Order Dependence

NO risk and vulnerabilities

Authorization through tx.origin

NO risk and vulnerabilities. tx.origin is not used on the contract

Block values as a proxy for time

NO risk and vulnerabilities.block.timestamp is not used on the contract.

Signature Malleability

NO risk and vulnerabilities.Does Not implement any signature verification on chain

Shadowing State Variables

NO risk and vulnerabilities.Even though the contract inherits ownable there aren't naming collisions

Weak Sources of Randomness from Chain Attributes

NO risk and vulnerabilities.does not generate any random numbers

Missing Protection against Signature Replay Attacks

NO risk and vulnerabilities.Does Not implement any signature verification on chain

Lack of Proper Signature Verification

NO risk and vulnerabilities.Does Not implement any signature verification on chain

Requirement Violation

NO risk and vulnerabilities.all the require statements are only placed to make sure that the corresponding function would not be functioning incase incorrect parameter values

Write to Arbitrary Storage Location

NO risk and vulnerabilities.This contract stores addresses of creator and owners of “SSID” on chain but only the current owners can actually has access to overwrite the value

Incorrect Inheritance Order

NO risk and vulnerabilities.It doesn’t implement Multi Inheritance.

Insufficient Gas Griefing

NO risk and vulnerabilities.There aren't any relay calls

Test Code Coverage

The test suite checks all the functions and covers 100 percent of the code.

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts/	100	100	100	100	
MultiSigWallet.sol	100	100	100	100	
All files	100	100	100	100	

Possible Deployment Issues

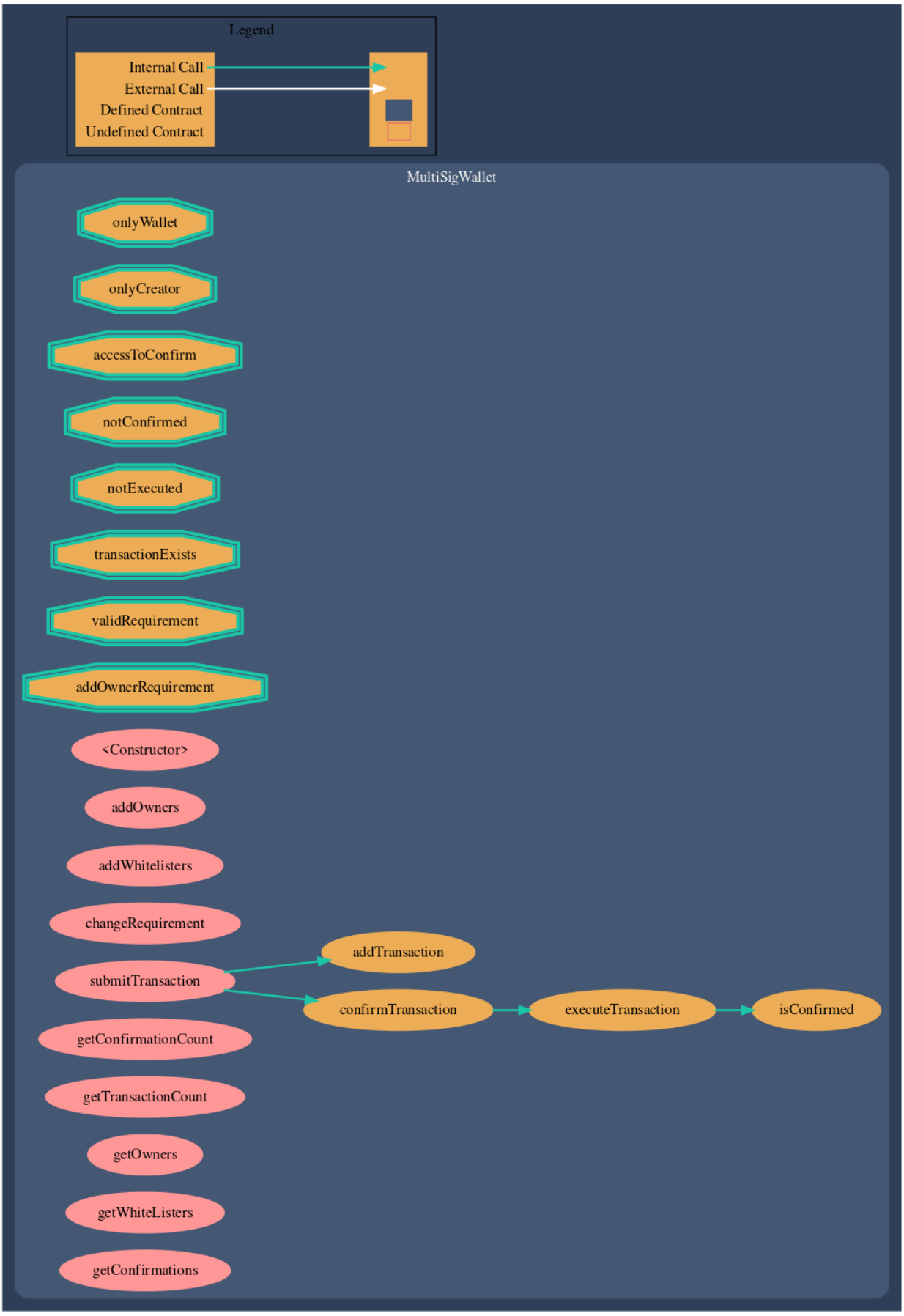
No issues with deployment when optimization is enabled with 200 runs

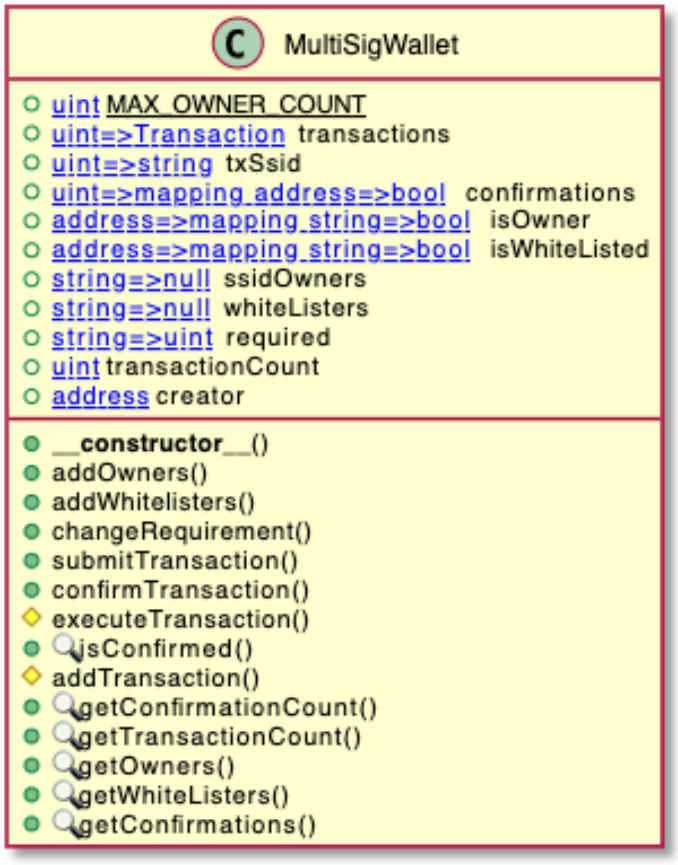
Possible Code Optimization

Code can be optimized by making variables with getter functions private

Smart Contract Visual Representation

Uml and flowchart of smart contract


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
MultiSigWallet
onlyWallet
onlyCreator
accessToConfirm
notConfirmed
notExecuted
transactionExists
validRequirement
addOwnerRequirement
<Constructor>
addOwners
addWhitelisters
changeRequirement
submitTransaction
addTransaction
confirmTransaction
executeTransaction
isConfirmed
getConfirmationCount
getTransactionCount
getOwners
getWhiteListers
getConfirmations



Results

Description Of Vulnerability	Risk Level
Function & State Variable Default Visibility	NA
Integer Overflow and Underflow	NA
Unchecked Call Return Value	NA
Unprotected Ether Withdrawal	NA
Unprotected Self Destruct Instruction	NA
Reentrancy Attack	NA
Uninitialized Storage Pointer	NA

Assert Violation	NA
Use of Deprecated Solidity Functions	NA
Delegatecall to Untrusted Callee	NA
DoS with Failed Call	NA
Transaction Order Dependence	NA
Authorization through tx.origin	NA
Block values as a proxy for time	NA
Signature Malleability	NA
Shadowing State Variables	NA
Weak Sources of Randomness from Chain Attributes	NA
Missing Protection against Signature Replay Attacks	NA
Lack of Proper Signature Verification	NA
Requirement Violation	NA
Write to Arbitrary Storage Location	NA
Incorrect Inheritance Order	NA
Insufficient Gas Griefing	NA

Final Report

The contract passes the audit with no critical issues or security concerns.