Checkout Smart Contracts Security Audit Scope.

Our Smart Contracts Security Audit process consists of the following stages:-

Stage 1 – Specification gathering

This is the most crucial stage because the detail is key for a successful smart contract Security audit. Here we will gather the specifications from you to know the intended behavior of smart contract. In this stage, we need a summary of the intended behavior of the smart contract from your side. We would also gather specification through forms.

You can provide specification summary in the form of example image attached below:-

Stage 2 – Manual Review

Manual Review is king in smart contract auditing

Goals of manual review:-

a.) Verify that every detail in the specification is implemented in smart contract.

b.) Verify that the contract does not have any behavior that is not specified in specifications.

c.) Verify that contract does not violate original intended behavior of specifications.

Here we would look for undefined, unexpected behavior and common security vulnerabilities like:-

=> Re-entrance
=> Overflows
=> Uncheck return values for low-level calls.
=> Denial of service
=> Bad randomness
=> Front running
=> Time manipulation
=> Short address attack
=> Unknown vulnerabilities

In manual review more that one auditor will review the code. The goal is to get to as many skilled eyes on contract code as possible.
Also, Read Our Next Article on QuillAudits.

=> We will apply all security attacks known till date on your contract manually to find security vulnerabilities

=> We will also ensure that your contract has some mechanism to defend against unknown vulnerabilities. Because the state of ethereum is constantly changing and we cannot say which vulnerabilities will arise in the future so we must have a mechanism beforehand.

=> We would ensure that smart contract code must respond to bugs and vulnerabilities well.

=> Manual testing will be done on test nets like rinkeby and ropsten.

=> We would also ensure that there is no unnecessary code in the contract.

=> Best code practices will also be considered in this phase.

Stage 3 – Unit testing

Goal:-Writing and running a comprehensive test suite.

=> In this stage smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.

=> In this phase intended behavior of smart contract is verified.

=> In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.

=> Gas limits of functions will be verified in this stage.

Stage 4 – Testing with automated tools

=> Testing with automated tools is important to catch those bugs that humans miss.

Some of the tools we would use are:-
Mythril
Oyente
Manticore
Solgraph
Solidity-coverage

At the end, we would provide you a comprehensive report along with details of audit and steps to cover up with the vulnerabilities if we found any in your contracts.