# 需提供资料：（名词写全称，不要简写）

1. **名词解释**

智能合约：存储在区块链系统中的计算机程序，程序的任何执行结果都记录在区块链上。（智能合约可代表法律上的合约条款，在满足条件时时强制且自动执行。）

形式化验证：,形式化验证是使用数学的形式化方法,证明或反驳系统所依据的预定算法在某种形式化规范或属性方面的正确性的行为。

1. **已知漏洞**

Smart Contract Weakness Classification（SWC，<https://swcregistry.io/>）列举了当前solidity语言智能合约中的安全漏洞。

Ethereum的GitHub仓库的Issue列表中（https://github.com/ethereum/ethereum-org-website/issues?q=is%3Aissue+is%3Aopen+label%3A%22bug+%3Abug%3A%22）列举了当前以太坊区块链系统中的安全漏洞。

IEEE的论文Potential risks of hyperledger fabric smart contracts中（https://ieeexplore.ieee.org/abstract/document/8666486）列举golang语言智能合约的安全漏洞。

1. **典型智能合约**

|  |  |  |
| --- | --- | --- |
| **序号** | **智能合约名称（加版本号）** | **下载地址** |
|  | XXX智能合约 V1.0 |  |

**451行 TetherToken**

[**https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7#code**](https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7#code)

**~~1652行 TRX~~**

[**~~https://etherscan.io/token/0x50327c6c5a14dcade707abad2e27eb517df87ab5#code~~**](https://etherscan.io/token/0x50327c6c5a14dcade707abad2e27eb517df87ab5#code)

**~~lscc.go 1156~~**

**~~paul-lee-attorney/fabric-2.1-gm core/scc/lscc/lscc.go~~**

**fabnode.go 696**

**amritpandey23/RPL-BlockTrust RPL\_BC\_Sandbox/artifacts/src/github.com/fabnode/go/fabnode.go**

1. **典型测试集**

|  |  |  |
| --- | --- | --- |
| **序号** | **智能合约名称** | **下载地址** |
|  |  |  |