ICS 35.240
L 70

DB43

湖　南　省　地　方　标　准

DB43/T 1839—2020

信息安全技术
区块链合约安全技术测评要求

Information security technology - Evaluation requirements for blockchain contract security technology

2020-09-30发布　　2020-12-30实施

湖南省市场监督管理局　发布

目　　次

前言…… III
1　范围…… 1
2　规范性引用文件…… 1
3　术语和定义 …… 1
4　等级测评概述…… 2
4.1　等级测评方法…… 2
4.2　单项测评…… 2
5　第一级测评要求…… 2
5.1　合约可终止性测评要求…… 2
5.2　合约确定性测评要求…… 3
5.3　合约可审计性测评要求…… 3
5.4　合约常用漏洞防护测评要求 …… 4
6　第二级测评要求…… 5
6.1　合约可终止性测评要求…… 5
6.2　合约确定性测评要求…… 6
6.3　合约可审计性测评要求…… 7
6.4　合约常用漏洞防护测评要求 …… 7
7　第三级测评要求…… 9
7.1　合约可终止性测评要求…… 9
7.2　合约确定性测评要求…… 10
7.3　合约可审计性测评要求…… 11
7.4　合约常用漏洞防护测评要求 …… 11
8　第四级测评要求…… 14
8.1　合约可终止性测评要求…… 14
8.2　合约确定性测评要求…… 15
8.3　合约可审计性测评要求…… 15
8.4　合约常用漏洞防护测评要求 …… 16
9　测评结论 …… 18
9.1　风险分析和评价 …… 18
9.2　等级测评结论…… 18
参考文献…… 20

前　言

本文件按照GB/T 1.1—2020给出的规则起草。

本文件由中共湖南省委网络安全和信息化委员会办公室提出。

本文件由湖南省区块链和分布式记账技术标准化技术委员会（筹）归口。

本文件起草单位：湖南链信安科技有限公司、湖南天河国云科技有限公司、湖南省东方区块链安全技术检测中心、湖南省人民政府发展研究中心、湖南天河云链科技有限公司。

本文件主要起草人：陈昕、谭林、杨征、梁亮、聂璐璐、梁琪、李财、聂朗、汪武、尹海波、黄帅、柳兴、郭慧、殷新文、丁雅琪、沈浪、张祥、宋姝、姜载乐、刘齐平、郑婷婷、胡钦、邹曼瑜等。

信息安全技术　区块链合约安全技术测评要求

1　范围

本文件规定了区块链合约安全技术测评指标要求。包括第一级、第二级、第三级和第四级区块链合约安全技术测评要求。

本文件适用于测评机构对区块链合约安全进行的测评工作，也适用于区块链技术开发者参考使用。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2010　信息安全技术　术语

GB/T 28458—2012　信息安全技术　安全漏洞标识与描述规范

3　术语和定义

GB/T 25069—2010、GB/T 28458—2012 界定的下列术语和定义适用于本文件。

3.1

智能合约　smart contracts

由事件驱动的、具有状态的、运行在可复制的共享区块链数据账本上的一段计算机代码，是现实世界中合约和规则的算法实现。

3.2

函数可重入　function reentrant

某函数被调用，没有执行完成，又一次被调用。

3.3

整数溢出　lnteger overflow

整数溢出漏洞包括上溢和下溢，上溢时指已经达到类型能表示的最大值后，再增加的话就会溢出，从一个很大的值变为 0，下溢是指已经是类型能表示的最小值，继续减小的话，就会变成一个很大的值。

3.4

安全审计　security audit

对信息系统的各种事件及行为实行监测、信息采集、分析，并针对特定事件及行为采取相应的动作。

[GB/T 25069—2010]

3.5

安全漏洞　vulnerability

计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

[GB/T 28458—2012]

4 等级测评概述

4.1 等级测评方法

等级测评实施的基本方法是针对待定的测评对象，采用相关的测评手段，遵从一定的测评规程，获取需要的证据数据，给出是否达到特定级别安全保护能力的评判。

本标准中针对每一个要求项的测评就构成一个单项测评，针对某个要求项的所有具体测评内容构成测评实施。根据调研结果，分析等级保护对象的业务流程和数据流，确定测评工作范围。结合等级保护对象的安全级别进行综合分析，测评对象可以根据类别加以描述，包括合约可终止性、合约确定性、合约可审计性、合约常用漏洞防护。

本标准账中每个级别测评要求都包括合约可终止性测评要求、合约确定性测评要求、合约可审计性测评要求、合约常用漏洞防护测评要求四部分内容。

4.2 单项测评

单项测评是针对各安全要求项的测评，支持测评结果的可重复性和可再现性。本标准中单项测评包括测评指标、测评对象、测评实施和测评判定结果构成。

5 第一级测评要求

5.1 合约可终止性测评要求

5.1.1 合约状态机

该测评单元包括以下要求：

a） 测评指标：合约应具有一种合适的确保合约不同状态暴露不同功能的状态机。

b） 测评对象：合约状态机。

c） 测评实施包括以下内容：

1） 是否支持合约的生命周期需要经历的所有阶段；

2） 是否支持合约的所有阶段的所有方法；

3） 阶段转换是否明确定义并对所有人公开；

4） 状态与状态之间的更新反应时间是否不超过 1 秒。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.1.2 合约资源控制

该测评单元包括以下要求：

a） 测评指标：合约应具有有效的资源管理模式保证合约可终止。

b） 测评对象：合约资源控制。

c） 测评实施包括以下内容：

1） 是否具有线性逻辑，资源必须且只能被使用一次；

2） 是否能够对资源进行合理的调配和部署；

3） 资源是否可以在有限时间内被释放。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.2 合约确定性测评要求

5.2.1 合约生命周期

该测评单元包括以下要求：

a） 测评指标：合约应具有一个完整的生命周期。

b） 测评对象：合约生命周期。

c） 测评实施包括以下内容：

1） 是否包括创建阶段；

2） 是否包括部署阶段；

3） 是否包括执行阶段；

4） 是否包括升级阶段；

5） 是否包括自毁阶段。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.3 合约可审计性测评要求

5.3.1 合约审计接口

该测评单元包括以下要求：

a） 测评指标：应提供合约部署、发布、执行审计接口。

b） 测评对象：合约审计接口。

c） 测评实施包括以下内容：

1） 是否具有部署审计接口；

2） 是否具有发布审计接口；

3） 是否具有执行审计接口。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.3.2 合约形式化验证

该测评单元包括以下要求：

a） 测评指标：应提供合约常规的形式化验证检测。

b） 测评对象：合约形式化验证。

c） 测评实施包括以下内容：

1） 是否进行合约代码规范验证；

2） 是否进行合约函数调用验证；

3） 是否进行合约业务逻辑安全验证；

4） 是否进行合约溢出验证检测；

5） 是否进行合约异常可达验证。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.4 合约常用漏洞防护测评要求

5.4.1 合约函数安全漏洞防护

该测评单元包括以下要求：

a） 测评指标：在使用了合约函数的情况下，合约应能防护函数安全漏洞。

b） 测评对象：合约函数安全漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否对调用请求的参数内容进行检测；

2） 是否确保调用前改变合约状态；

3） 是否引入互斥锁。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.4.2 合约条件竞争漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护条件竞争漏洞。

b） 测评对象：条件竞争漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否针对接受者账户进行效验；

2） 是否针对传输的通证数量进行检查；

3） 是否在逻辑中设置实际工作量上限。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.4.3 合约重入攻击漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护重入攻击漏洞。

b） 测评对象：重入攻击漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用转账函数；

2） 是否确保在使用转账函数之前改变合约状态；

3） 是否引入互斥锁。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.4.4 合约权限控制漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护权限控制漏洞。

b） 测评对象：权限控制漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否设置为仅所有者用户有自毁权限；

2） 是否对转账操作添加权限修饰；

3） 是否对于具有修改能力的函数添加相应的权限修饰符；

4） 是否在授权时不使用类似于 tx.origin 的全局变量。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.4.5 合约事务顺序依赖漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护事务顺序依赖漏洞。

b） 测评对象：事务顺序依赖漏洞防护方法。

c） 测评实施包括以下内容：

1） 智能合约的执行是否不随着事务处理的顺序不同而产生差异。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.4.6 合约逻辑设计缺陷漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护逻辑设计缺陷漏洞。

b） 测评对象：逻辑设计缺陷漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否在使用用户传入的参数之前首先进行相应的检测；

2） 是否具备错误或异常的处理机制；

3） 是否具有支持日志的数据结构。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.4.7 合约错误使用随机数漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护错误使用随机数漏洞。

b） 测评对象：错误使用随机数漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用安全的随机数产生方法。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6 第二级测评要求

6.1 合约可终止性测评要求

6.1.1 合约状态机

该测评单元包括以下要求：

a） 测评指标：合约应具有一种合适的确保合约不同状态暴露不同功能的状态机。

b） 测评对象：合约状态机。

c） 测评实施包括以下内容：
1） 是否支持合约的生命周期需要经历的所有阶段；
2） 是否支持合约的所有阶段的所有方法；
3） 阶段转换是否明确定义并对所有人公开；
4） 状态与状态之间的更新反应时间是否不超过 1 秒。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.2 合约资源控制

该测评单元包括以下要求：
a） 测评指标：合约应具有有效的资源管理模式保证合约可终止。
b） 测评对象：合约资源控制。
c） 测评实施包括以下内容：
1） 是否具有线性逻辑，资源必须且只能被使用一次；
2） 是否能够对资源进行合理的调配和部署；
3） 资源是否可以在有限时间内被释放。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3 合约访问控制

该测评单元包括以下要求：
a） 测评指标：合约应具有默认的属性权限和访问控制机制。
b） 测评对象：合约访问控制。
c） 测评实施包括以下内容：
1） 属性权限是否具有类似公开、保护、私有的分级；
2） 是否只有是公开类型时，才可以通过合约地址进行访问；
3） 是否合约内部要访问内部类型和私有类型的属性和方法时，直接访问即可，合约外部无法访问私有类型的属性和方法；
4） 是否用外部类型声明的合约成员可以被其他合约和交易直接调用。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.2 合约确定性测评要求

6.2.1 合约生命周期

该测评单元包括以下要求：
a） 测评指标：合约应具有一个完整的生命周期。
b） 测评对象：合约生命周期。
c） 测评实施包括以下内容：
1） 是否包括创建阶段；
2） 是否包括部署阶段；
3） 是否包括执行阶段；

4） 是否包括升级阶段；
5） 是否包括自毁阶段。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3 合约可审计性测评要求

6.3.1 合约审计接口

该测评单元包括以下要求：

a） 测评指标：应提供合约部署、发布、执行审计接口。
b） 测评对象：合约审计接口。
c） 测评实施包括以下内容：
1） 是否具有部署审计接口；
2） 是否具有发布审计接口；
3） 是否具有执行审计接口。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.2 合约形式化验证

该测评单元包括以下要求：

a） 测评指标：应提供合约常规的形式化验证检测。
b） 测评对象：合约形式化验证。
c） 测评实施包括以下内容：
1） 是否进行合约代码规范验证；
2） 是否进行合约函数调用验证；
3） 是否进行合约业务逻辑安全验证；
4） 是否进行合约溢出验证检测；
5） 是否进行合约异常可达验证。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4 合约常用漏洞防护测评要求

6.4.1 合约函数安全漏洞防护

该测评单元包括以下要求：

a） 测评指标：在使用了合约函数的情况下，合约应能防护函数安全漏洞。
b） 测评对象：合约函数安全漏洞防护方法。
c） 测评实施包括以下内容：
1） 是否对调用请求的参数内容进行检测；
2） 是否确保调用前改变合约状态；
3） 是否引入互斥锁。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.2 合约条件竞争漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护条件竞争漏洞。

b） 测评对象：条件竞争漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否针对接受者账户进行效验；

2） 是否针对传输的通证数量进行检查；

3） 是否在逻辑中设置实际工作量上限。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.3 合约重入攻击漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护重入攻击漏洞。

b） 测评对象：重入攻击漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用转账函数；

2） 是否确保在使用转账函数之前改变合约状态；

3） 是否引入互斥锁。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.4 合约权限控制漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护权限控制漏洞。

b） 测评对象：权限控制漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否设置为仅所有者用户有自毁权限；

2） 是否对转账操作添加权限修饰；

3） 是否对于具有修改能力的函数添加相应的权限修饰符；

4） 是否在授权时未使用类似于 tx.origin 的全局变量。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.5 合约数值溢出漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护数值溢出漏洞。

b） 测评对象：数值溢出漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用防止溢出和下溢的数学运算库进行安全的算术操作。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评

单元指标要求。

6.4.6 合约事务顺序依赖漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护事务顺序依赖漏洞。

b） 测评对象：事务顺序依赖漏洞防护方法。

c） 测评实施包括以下内容：

1） 智能合约的执行是否不随着事务处理的顺序不同而产生差异。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7 合约逻辑设计缺陷漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护逻辑设计缺陷漏洞。

b） 测评对象：逻辑设计缺陷漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否在使用用户传入的参数之前首先进行相应的检测；

2） 是否具备错误或异常的处理机制；

3） 是否具有支持日志的数据结构。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.8 合约错误使用随机数漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护错误使用随机数漏洞。

b） 测评对象：错误使用随机数漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用安全的随机数产生方法。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7 第三级测评要求

7.1 合约可终止性测评要求

7.1.1 合约状态机

该测评单元包括以下要求：

a） 测评指标：合约应具有一种合适的确保合约不同状态暴露不同功能的状态机。

b） 测评对象：合约状态机。

c） 测评实施包括以下内容：

1） 是否支持合约的生命周期需要经历的所有阶段；

2） 是否支持合约的所有阶段的所有方法；

3） 阶段转换是否明确定义并对所有人公开；
4） 状态与状态之间的更新反应时间是否不超过 1 秒。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2 合约资源控制

该测评单元包括以下要求：

a） 测评指标：合约应具有有效的资源管理模式保证合约可终止。
b） 测评对象：合约资源控制。
c） 测评实施包括以下内容：
1） 是否具有线性逻辑，资源必须且只能被使用一次；
2） 是否能够对资源进行合理的调配和部署；
3） 资源是否可以在有限时间内被释放；
4） 合约是否必须在有限时间内完成运行。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3 合约访问控制

该测评单元包括以下要求：

a） 测评指标：合约应具有默认的属性权限和访问控制机制。
b） 测评对象：合约访问控制。
c） 测评实施包括以下内容：
1） 属性权限是否具有类似公开、保护、私有的分级；
2） 是否只有是公开类型时，才可以通过合约地址进行访问；
3） 是否合约内部要访问内部类型和私有类型的属性和方法时，直接访问即可，合约外部无法访问私有类型的属性和方法；
4） 是否用外部类型声明的合约成员可以被其他合约和交易直接调用；
5） 是否用内部类型声明的函数和变量只能在内部使用，但可以继承。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2 合约确定性测评要求

7.2.1 合约通证标准

该测评单元包括以下要求：

a） 测评指标：合约应为通证发行提供一个特征与接口的共同标准。
b） 测评对象：合约通证标准。
c） 测评实施包括以下内容：
1） 如果支持支付类通证，是否提供支付类通证标准；
2） 如果支持实用类通证，是否提供实用类通证标准；
3） 如果支持资产类通证，是否提供资产类通证标准。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分

符合本测评单元指标要求。

7.2.2 合约生命周期

该测评单元包括以下要求：

a） 测评指标：合约应具有一个完整的生命周期。

b） 测评对象：合约生命周期。

c） 测评实施包括以下内容：

1） 是否包括创建阶段；

2） 是否包括部署阶段；

3） 是否包括执行阶段；

4） 是否包括升级阶段；

5） 是否包括自毁阶段。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3 合约可审计性测评要求

7.3.1 合约审计接口

该测评单元包括以下要求：

a） 测评指标：应提供合约部署、发布、执行审计接口。

b） 测评对象：合约审计接口。

c） 测评实施包括以下内容：

1） 是否具有部署审计接口；

2） 是否具有发布审计接口；

3） 是否具有执行审计接口。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.2 合约形式化验证

该测评单元包括以下要求：

a） 测评指标：应提供合约常规的形式化验证检测。

b） 测评对象：合约形式化验证。

c） 测评实施包括以下内容：

1） 是否进行合约代码规范验证；

2） 是否进行合约函数调用验证；

3） 是否进行合约业务逻辑安全验证；

4） 是否进行合约溢出验证检测；

5） 是否进行合约异常可达验证；

6） 是否进行自动代码生成和一致化验证。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4 合约常用漏洞防护测评要求

7.4.1 合约函数安全漏洞防护

该测评单元包括以下要求：

a） 测评指标：在使用了合约函数的情况下，合约应能防护函数安全漏洞。

b） 测评对象：合约函数安全漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否对调用请求的参数内容进行检测；

2） 是否确保调用前改变合约状态；

3） 是否引入互斥锁。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.2 合约条件竞争漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护条件竞争漏洞。

b） 测评对象：条件竞争漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否针对接受者账户进行效验；

2） 是否针对传输的通证数量进行检查；

3） 是否在逻辑中设置实际工作量上限。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.3 合约重入攻击漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护重入攻击漏洞。

b） 测评对象：重入攻击漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用转账函数；

2） 是否确保在使用转账函数之前改变合约状态；

3） 是否引入互斥锁。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.4 合约权限控制漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护权限控制漏洞。

b） 测评对象：权限控制漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否设置为仅所有者用户有自毁权限；

2） 是否对转账操作添加权限修饰；

3） 是否对于具有修改能力的函数添加相应的权限修饰符；

4） 是否在授权时未使用类似于 tx.origin 的全局变量。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.5 合约数值溢出漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护数值溢出漏洞。

b） 测评对象：数值溢出漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用防止溢出和下溢的数学运算库进行安全的算术操作。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.4.6 合约事务顺序依赖漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护事务顺序依赖漏洞。

b） 测评对象：事务顺序依赖漏洞防护方法。

c） 测评实施包括以下内容：

1） 智能合约的执行是否不随着事务处理的顺序不同而产生差异。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.4.7 合约账户冻结及绕过漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护账户冻结及绕过漏洞。

b） 测评对象：账户冻结及绕过漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否做好函数存取款逻辑的检查。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.4.8 合约逻辑设计缺陷漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护逻辑设计缺陷漏洞。

b） 测评对象：逻辑设计缺陷漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否在使用用户传入的参数之前首先进行相应的检测；

2） 是否具备错误或异常的处理机制；

3） 是否具有支持日志的数据结构。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.9 合约错误使用随机数漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护错误使用随机数漏洞。

b） 测评对象：错误使用随机数漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用安全的随机数产生方法。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8 第四级测评要求

8.1 合约可终止性测评要求

8.1.1 合约状态机

该测评单元包括以下要求：

a） 测评指标：合约应具有一种合适的确保合约不同状态暴露不同功能的状态机。

b） 测评对象：合约状态机。

c） 测评实施包括以下内容：

1） 是否支持合约的生命周期需要经历的所有阶段；

2） 是否支持合约的所有阶段的所有方法；

3） 阶段转换是否明确定义并对所有人公开；

4） 状态与状态之间的更新反应时间是否不超过 1 秒。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2 合约资源控制

该测评单元包括以下要求：

a） 测评指标：合约应具有有效的资源管理模式保证合约可终止。

b） 测评对象：合约资源控制。

c） 测评实施包括以下内容：

1） 是否具有线性逻辑，资源必须且只能被使用一次；

2） 是否能够对资源进行合理的调配和部署；

3） 资源是否可以在有限时间内被释放；

4） 合约是否必须在有限时间内完成运行。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3 合约访问控制

该测评单元包括以下要求：

a） 测评指标：合约应具有默认的属性权限和访问控制机制。

b） 测评对象：合约访问控制。

c） 测评实施包括以下内容：

1） 属性权限是否具有类似公开、保护、私有的分级；

2） 是否只有是公开类型时，才可以通过合约地址进行访问；
3） 是否合约内部要访问内部类型和私有类型的属性和方法时，直接访问即可，合约外部无法访问私有类型的属性和方法；
4） 是否用外部类型声明的合约成员可以被其他合约和交易直接调用；
5） 是否用内部类型声明的函数和变量只能在内部使用，但可以继承。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.2 合约确定性测评要求

8.2.1 合约通证标准

该测评单元包括以下要求：

a） 测评指标：合约应为通证发行提供一个特征与接口的共同标准。
b） 测评对象：合约通证标准。
c） 测评实施包括以下内容：
1） 如果支持支付类通证，是否提供支付类通证标准；
2） 如果支持实用类通证，是否提供实用类通证标准；
3） 如果支持资产类通证，是否提供资产类通证标准。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.2.2 合约生命周期

该测评单元包括以下要求：

a） 测评指标：合约应具有一个完整的生命周期。
b） 测评对象：合约生命周期。
c） 测评实施包括以下内容：
1） 是否包括创建阶段；
2） 是否包括部署阶段；
3） 是否包括执行阶段；
4） 是否包括升级阶段；
5） 是否包括自毁阶段。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3 合约可审计性测评要求

8.3.1 合约审计接口

该测评单元包括以下要求：

a） 测评指标：应提供合约部署、发布、执行的审计接口。
b） 测评对象：合约审计接口。
c） 测评实施包括以下内容：
1） 是否具有部署审计接口；

2） 是否具有发布审计接口；
3） 是否具有执行审计接口；
4） 是否内嵌自助审计工具。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2 合约形式化验证

该测评单元包括以下要求：

a） 测评指标：应提供合约常规的形式化验证检测。
b） 测评对象：合约形式化验证。
c） 测评实施包括以下内容：
1） 是否进行合约代码规范验证；
2） 是否进行合约函数调用验证；
3） 是否进行合约业务逻辑安全验证；
4） 是否进行合约溢出验证检测；
5） 是否进行合约异常可达验证；
6） 是否进行自动代码生成和一致化验证；
7） 是否进行演绎验证-逻辑公式描述流程检查。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4 合约常用漏洞防护测评要求

8.4.1 合约函数安全漏洞防护

该测评单元包括以下要求：

a） 测评指标：在使用了合约函数的情况下，合约应能防护函数安全漏洞。
b） 测评对象：合约函数安全漏洞防护方法。
c） 测评实施包括以下内容：
1） 是否对调用请求的参数内容进行检测；
2） 是否确保调用前改变合约状态；
3） 是否引入互斥锁。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.2 合约条件竞争漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护条件竞争漏洞。
b） 测评对象：条件竞争漏洞防护方法。
c） 测评实施包括以下内容：
1） 是否针对接受者账户进行效验；
2） 是否针对传输的通证数量进行检查；
3） 是否在逻辑中设置实际工作量上限。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3 合约重入攻击漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护重入攻击漏洞。

b） 测评对象：重入攻击漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用转账函数；

2） 是否确保在使用转账函数之前改变合约状态；

3） 是否引入互斥锁。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.4 合约权限控制漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护权限控制漏洞。

b） 测评对象：权限控制漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否设置为仅所有者用户有自毁权限；

2） 是否对转账操作添加权限修饰；

3） 是否对于具有修改能力的函数添加相应的权限修饰符；

4） 是否在授权时不使用类似于 tx.origin 的全局变量。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.5 合约数值溢出漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护数值溢出漏洞。

b） 测评对象：数值溢出漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用防止溢出和下溢的数学运算库进行安全的算术操作。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.4.6 合约事务顺序依赖漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护事务顺序依赖漏洞。

b） 测评对象：事务顺序依赖漏洞防护方法。

c） 测评实施包括以下内容：

1） 智能合约的执行是否不随着事务处理的顺序不同而产生差异。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评

单元指标要求。

8.4.7 合约账户冻结及绕过漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护账户冻结及绕过漏洞。

b） 测评对象：账户冻结及绕过漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否做好函数存取款逻辑的检查。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.4.8 合约逻辑设计缺陷漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护逻辑设计缺陷漏洞。

b） 测评对象：逻辑设计缺陷漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否在使用用户传入的参数之前首先进行相应的检测；

2） 是否具备错误或异常的处理机制；

3） 是否具有支持日志的数据结构。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.9 合约错误使用随机数漏洞防护

该测评单元包括以下要求：

a） 测评指标：合约能够防护错误使用随机数漏洞。

b） 测评对象：错误使用随机数漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否使用安全的随机数产生方法。

d） 测评判定：如果以上测评实施内容全为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9 测评结论

9.1 风险分析和评价

等级测评报告中应对整体测评之后单项测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法对单项测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度，综合评价这些不符合项或部分符合项对定级对象造成的安全风险。风险分析和评价应根据特定的条件和场景下展开，并对高风险的测试项予以预警。

9.2 等级测评结论

应结合各类的测评结论和对单项测评结果的风险分析给出等级测评结论：

a） 符合：定级对象中未发现安全问题，等级测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果全为0。

b） 基本符合：定级对象中存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题不会导致定级对象面临高等级安全风险。

c） 不符合：定级对象中存在安全问题，部分符合项和不符合项的统计结果不全为0，而且存在的安全问题会导致定级对象面临高等级安全风险。

参 考 文 献

[1] GB/T 25069—2010 信息安全技术 术语.

[2] GB/T 33561—2017 信息安全技术 安全漏洞分类.

[3] 付梦琳，吴礼发，洪征，等. 智能合约安全漏洞挖掘技术研究[J]. 计算机应用，2019，39(7)：1959-1966.

[4] 邱欣欣，马兆丰，徐明昆. 以太坊智能合约安全漏洞分析及对策[J]. 信息安全与通信保密，2019，302(02):46-55.

[5] Manning A. Solidity security: Comprehensive list of known attack vectors and common anti-patterns[J]. Sigma Prime, 2018, 20(10).