ICS 35.240
L 70

# DB43

# 湖　南　省　地　方　标　准

DB43/T 1842—2020

# 信息安全技术
# 区块链应用安全技术测评要求

Information security technology - Evaluation requirements for blockchain application 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

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：谭林、聂朗、梁琪、杨征、陈昕、李财、聂璐璐、梁亮、尹海波、黄帅、汪武、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　区块链应用安全技术测评要求

## 1　范围

本文件规定了区块链应用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应用安全技术测评要求。

本文件适用于测评机构对区块链应用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

**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]

3.2

**访问控制　access level**

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

[GB/T 25069—2010]

3.3

**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]

3.4

**联盟链　consortium blockchain**

联盟链是一种共识过程受到预先设定节点控制的区块链类型，只限于预先选定的联盟成员参与，每个联盟成员作为一个节点，各个节点在链上的权限按联盟共同制定的规则来设定。

3.5

**私有链　private blockchain**

私有链是一种中心化的区块链类型，它所有的权限由这个中心化的组织和机构来控制。

# 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，包括业务平台安全、漏洞防护、安全审计。

本标准账中每个级别测评要求都包括业务平台安全测评要求、漏洞防护测评要求、安全审计测评要求三部分内容。

## 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 应用系统测评要求

### 5.1.1 用户身份鉴别

该测评单元包括以下要求：

a） 测评指标：应保证用户身份被安全认证，且具有唯一标识特性。

b） 测评对象：用户身份认证机制。

c） 测评实施包括以下内容：

1） 用户身份标识是否具有唯一性，身份鉴别信息定期更换；

2） 是否具备对同一用户采用两种或以上组合的身份认证技术，实现多因子用户身份认证，包括但不限于密钥、登录码、手机动态码等方式。

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 访问控制

该测评单元包括以下要求：

a） 测评指标：应保证区块链系统具备有效的访问控制策略。

b） 测评对象：访问控制策略。

c） 测评实施包括以下内容：

1） 是否按照权限最小化、相互制约原则，为用户分配访问权限；

2） 每个用户交互时是否均检测其访问控制状态。

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。

#### 5.1.3 配置管理

该测评单元包括以下要求：

a） 测评指标：应提供安全配置策略。

b） 测评对象：配置信息。

c） 测评实施包括以下内容：

1） 是否提供配置管理功能，对所有配置项进行维护，并唯一标识配置项。

d） 测评判定：如果以上测评实施内容为肯定，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。

### 5.2 漏洞防护测评要求

#### 5.2.1 系统配置类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对安全配置等系统配置类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 开发环境、预发布环境和生产环境是否配置相同，且使用不同的密码；

2） 在各组件之间是否提供一种应用程序框架，可提供有效的组件分离和安全性保障功能。

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。

#### 5.2.2 访问控制类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对功能级访问控制缺失等访问控制类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否设置检测攻击机制，例如检测合法用户无法正常输入、异常使用、重复请求等。

d） 测评判定：如果以上测评实施内容为肯定，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。

#### 5.2.3 数据泄露类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对敏感数据泄露等数据泄露类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 针对没必要存放的、重要的敏感数据，是否设置清除机制。

d） 测评判定：如果以上测评实施内容为肯定，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。

### 5.3 安全审计测评要求

#### 5.3.1 审计功能

该测评单元包括以下要求：

a） 测评指标：应提供覆盖到每个用户的安全审计功能，对应用的重要安全事件进行审计。
b） 测评对象：安全审计功能。
c） 测评实施包括以下内容：
1） 是否提供覆盖到每个用户的安全审计功能；
2） 是否对应用的重要安全事件进行审计，且对安全事件进行提醒或告警处理。
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 审计进程及记录

该测评单元包括以下要求：
a） 测评指标：应确保无法单独中断审计进程。
b） 测评对象：审计记录控制功能。
c） 测评实施包括以下内容：
1） 是否无法单独中断审计进程。
d） 测评判定：如果以上测评实施内容为肯定，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。

#### 5.3.3 审计记录内容

该测评单元包括以下要求：
a） 测评指标：应保证审计记录的内容包括事件时间、内容、发起者信息。
b） 测评对象：审计记录内容。
c） 测评实施包括以下内容：
1） 审计记录的内容是否包括事件时间；
2） 审计记录的内容是否包括事件内容；
3） 审计记录的内容是否包括事件发起者信息。
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。

#### 5.3.4 活动审计

该测评单元包括以下要求：
a） 测评指标：应保证活动审计具备完整阶段、覆盖全面的审计指标。
b） 测评对象：区块链活动审计功能。
c） 测评实施包括以下内容：
1） 是否对区块链活动的事前、事中、事后三个阶段进行审计；
2） 是否包含查处违规违纪审计、内控制度审计、绩效审计等审计指标。
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。

#### 5.3.5 审计日志

该测评单元包括以下要求：
a） 测评指标：应保证审计日志内容的完整性。
b） 测评对象：审计日志。

c） 测评实施包括以下内容：

1） 是否保存与审计活动相关的运营环境条件的记录和日志。

d） 测评判定：如果以上测评实施内容为肯定，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 应用系统测评要求

#### 6.1.1 用户身份鉴别

该测评单元包括以下要求：

a） 测评指标：应保证用户身份被安全认证，且具有唯一标识特性。

b） 测评对象：用户身份认证及鉴别机制。

c） 测评实施包括以下内容：

1） 用户身份标识是否具有唯一性；

2） 是否具备对同一用户采用两种或以上组合的身份认证技术，实现多因子用户身份认证，包括但不限于密钥、登录码、手机动态码等方式；

3） 是否具备用户身份标识和鉴别信息复杂度检查功能。

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 访问控制

该测评单元包括以下要求：

a） 测评指标：应保证区块链系统具备安全、有效的访问控制策略。

b） 测评对象：访问控制策略。

c） 测评实施包括以下内容：

1） 是否按照权限最小化、相互制约原则，为用户分配访问权限；

2） 每个用户交互时是否均检测其访问控制状态。

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 配置管理

该测评单元包括以下要求：

a） 测评指标：应具备安全配置管理策略。

b） 测评对象：配置信息。

c） 测评实施包括以下内容：

1） 是否提供配置管理功能，对所有配置项进行维护，并唯一标识配置项；

2） 是否提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法。

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。

#### 6.1.4 备份与故障恢复

该测评单元包括以下要求：

a） 测评指标：应提供完善的系统备份与故障恢复机制。

b） 测评对象：备份与故障恢复机制。

c） 测评实施包括以下内容：

1） 应用系统是否提供数据备份与恢复机制；

2） 是否为系统配置、用户敏感信息等重要数据提供多种备份方式；

3） 是否为用户提供自主选择备份重要信息的功能。

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。

#### 6.1.5 系统异常处理

该测评单元包括以下要求：

a） 测评指标：系统针对异常登录、错误信息等情况应具备异常处理功能。

b） 测评对象：系统异常情况处理机制。

c） 测评实施包括以下内容：

1） 是否提供登录异常处理功能，例如采取结束会话、限制非法登录次数、自动退出或者采用多重认证等手段增强身份验证等措施；

2） 在认证反复出现错误时是否有账户安全警告与锁定功能；

3） 在针对账号信息遗忘等情况是否具备可靠的找回机制。

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 漏洞防护测评要求

#### 6.2.1 注入类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对 SQL 注入、OS 命令注入等注入类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 若未使用参数化的应用程序接口，是否使用解释器来避免特殊字符的出现；

2） 是否使用正面或“白名单”中恰当的、规范化的输入验证方法防止注入类攻击；

3） 在区块链项目的 web 端，是否避免动态调用智能合约。

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。

#### 6.2.2 跨站类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对跨站脚本、跨站请求伪造等跨站类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 查看是否每个链接和表单都提供了不可预测的跨站请求伪造令牌；

2） 是否采用内容安全策略，将不可信数据与动态的浏览器内容区分开，来抵御整个系统的跨

站脚本攻击；

3） 应用程序接口是否具备身份验证方案，并且所有凭据、密钥和令牌均已被保护。

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。

#### 6.2.3 系统配置类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对安全配置等系统配置类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 开发环境、预发布环境和生产环境是否配置相同，且使用不同的密码；

2） 在各组件之间是否提供一种应用程序框架，可提供有效的组件分离和安全性保障功能；

3） 区块链的联盟链或私有链是否配置加固的、标准的节点，且不允许没有加固的、非标准的服务器成为区块链的节点。

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。

#### 6.2.4 访问控制类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对功能级访问控制缺失等访问控制类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否设置检测攻击机制，例如检测合法用户无法正常输入、异常使用、重复请求等；

2） 是否自动阻止异常请求，禁用或监控不良行为的用户账户。

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。

#### 6.2.5 数据泄露类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对敏感数据泄露等数据泄露类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 针对没必要存放的、重要的敏感数据，是否设置清除机制；

2） 是否禁止自动完成功能以防止敏感数据收集，禁用包含敏感数据的缓存页面。

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 安全审计测评要求

#### 6.3.1 审计功能

该测评单元包括以下要求：

a） 测评指标：应提供覆盖到每个用户的安全审计功能，对应用的重要安全事件进行审计。

b） 测评对象：审计功能。

c） 测评实施包括以下内容：
1） 是否提供覆盖到每个用户的安全审计功能；
2） 是否对应用的重要安全事件进行审计，且对安全事件进行提醒或告警处理。
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 审计进程及记录

该测评单元包括以下要求：
a） 测评指标：应确保无法单独中断审计进程，无法删除、修改或覆盖审计记录。
b） 测评对象：审计进程及记录。
c） 测评实施包括以下内容：
1） 是否无法单独中断审计进程；
2） 是否无法删除审计记录；
3） 是否无法修改审计记录；
4） 是否无法覆盖审计记录。
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。

### 6.3.3 审计记录内容

该测评单元包括以下要求：
a） 测评指标：审计记录的内容应包括事件时间、内容、发起者信息、类型。
b） 测评对象：审计记录内容。
c） 测评实施包括以下内容：
1） 审计记录的内容是否包括事件时间；
2） 审计记录的内容是否包括事件内容；
3） 审计记录的内容是否包括事件发起者信息；
4） 审计记录的内容是否包括事件类型。
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。

### 6.3.4 活动审计

该测评单元包括以下要求：
a） 测评指标：应保证活动审计具备完整阶段、覆盖全面的审计指标。
b） 测评对象：区块链活动审计功能。
c） 测评实施包括以下内容：
1） 是否对区块链活动的事前、事中、事后三个阶段进行审计；
2） 是否包含查处违规违纪审计、内控制度审计、绩效审计等审计指标；
3） 是否实现区块链服务审计方加入区块链网络作为其中一个节点进行实时审计。
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。

### 6.3.5 审计日志

该测评单元包括以下要求：

a） 测评指标：应保证审计日志记录功能完善。

b） 测评对象：审计日志。

c） 测评实施包括以下内容：

1） 是否保存与审计活动相关的运营环境条件的记录和日志；

2） 是否保存审计员的审计查看动作记录。

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 第三级测评要求

## 7.1 应用系统测评要求

### 7.1.1 用户身份鉴别

该测评单元包括以下要求：

a） 测评指标：应保证用户身份标识具有唯一性，且用户身份可被安全认证，保证身份鉴别信息的安全性。

b） 测评对象：用户身份认证及鉴别机制。

c） 测评实施包括以下内容：

1） 用户身份标识是否具有唯一性；

2） 是否具备对同一用户采用两种或以上组合的身份认证技术，实现多因子用户身份认证，包括但不限于密钥、登录码、手机动态码等方式；

3） 是否具备用户身份标识和鉴别信息复杂度检查功能；

4） 是否建立以数字证书为核心的身份认证系统，以安全保密方式实现用户身份鉴别。

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 访问控制

该测评单元包括以下要求：

a） 测评指标：应保证区块链系统具备安全、有效的访问控制策略。

b） 测评对象：访问控制策略。

c） 测评实施包括以下内容：

1） 是否按照权限最小化、相互制约原则，为用户分配访问权限；

2） 每个用户交互时是否均检测其访问控制状态；

3） 是否只有授权用户才具备访问秘密数据或敏感数据权限，并且不能越级访问，例如与用户信息或系统自身安全密切相关的状态信息、文件或其他资源、受保护的功能以及与安全相关的配置信息等。

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 配置管理

该测评单元包括以下要求：

a） 测评指标：应具备安全配置管理策略。
b） 测评对象：配置信息。
c） 测评实施包括以下内容：
1） 是否提供配置管理功能，对所有配置项进行维护，并唯一标识配置项；
2） 是否提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
3） 配置信息的变更是否具有相应的申报审批程序。
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。

#### 7.1.4 备份与故障恢复

该测评单元包括以下要求：
a） 测评指标：应提供完善的系统备份与故障恢复机制。
b） 测评对象：备份与故障恢复机制。
c） 测评实施包括以下内容：
1） 应用系统是否提供数据备份与恢复机制；
2） 是否为系统配置、用户敏感信息等重要数据提供多种备份方式；
3） 是否为用户提供自主选择备份重要信息的功能；
4） 数据恢复后，系统是否进行校验，且可以正常运行。
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。

#### 7.1.5 系统异常处理

该测评单元包括以下要求：
a） 测评指标：系统针对异常登录、错误信息等情况应具备异常处理功能。
b） 测评对象：系统异常情况处理机制。
c） 测评实施包括以下内容：
1） 是否提供登录异常处理功能，例如采取结束会话、限制非法登录次数、自动退出或者采用多重认证等手段增强身份验证等措施；
2） 在认证反复出现错误时是否有账户安全警告与锁定功能；
3） 在针对账号信息遗忘等情况是否具备可靠的找回机制。
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 漏洞防护测评要求

#### 7.2.1 注入类漏洞防护

该测评单元包括以下要求：
a） 测评指标：针对 SQL 注入、OS 命令注入等注入类漏洞，应具备安全防护措施。
b） 测评对象：漏洞防护方法。
c） 测评实施包括以下内容：
1） 若未使用参数化的应用程序接口，是否使用解释器来避免特殊字符的出现；
2） 是否使用正面或“白名单”中恰当的、规范化的输入验证方法防止注入类攻击；

3） 在区块链项目的web端，是否避免动态调用智能合约。

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 跨站类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对跨站脚本、跨站请求伪造等跨站类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 查看是否每个链接和表单都提供了不可预测的跨站请求伪造令牌；

2） 是否采用内容安全策略，将不可信数据与动态的浏览器内容区分开，来抵御整个系统的跨站脚本攻击；

3） 应用程序接口是否具备身份验证方案，并且所有凭据、密钥和令牌均已被保护；

4） 是否建立应用程序接口调用的访问控制机制和加密策略，防止跨站类漏洞攻击。

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。

#### 7.2.3 系统配置类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对安全配置等系统配置类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 开发环境、预发布环境和生产环境是否配置相同，且使用不同的密码；

2） 在各组件之间是否提供一种应用程序框架，可提供有效的组件分离和安全性保障功能；

3） 区块链的联盟链或私有链是否配置加固的、标准的节点，且不允许没有加固的、非标准的服务器成为区块链的节点；

4） 是否设置自动化过程来验证所有环境中配置信息的正确性。

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。

#### 7.2.4 访问控制类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对功能级访问控制缺失等访问控制类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否设置检测攻击机制，例如检测合法用户无法正常输入、异常使用、重复请求等；

2） 是否自动阻止异常请求，禁用或监控不良行为的用户账户；

3） 是否采用特殊的智能合约来判断不正常的用户行为，并且在发现紧急安全问题时，允许智能合约的拥有者停止智能合约的运行，或者运行智能合约自动采取措施停止运行。

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。

#### 7.2.5 数据泄露类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对敏感数据泄露等数据泄露类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 针对没必要存放的、重要的敏感数据，是否设置清除机制；

2） 是否禁止自动完成功能以防止敏感数据收集，禁用包含敏感数据的缓存页面；

3） 在公有链上是否避免存储敏感数据。

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 安全审计测评要求

#### 7.3.1 审计功能

该测评单元包括以下要求：

a） 测评指标：应提供覆盖到每个用户的安全审计功能，对应用的重要安全事件进行审计。

b） 测评对象：安全审计功能。

c） 测评实施包括以下内容：

1） 是否提供覆盖到每个用户的安全审计功能；

2） 是否对应用的重要安全事件进行审计，且对安全事件进行提醒或告警处理。

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 审计进程及记录

该测评单元包括以下要求：

a） 测评指标：应确保无法单独中断审计进程，无法删除、修改或覆盖审计记录。

b） 测评对象：审计进程及记录。

c） 测评实施包括以下内容：

1） 是否无法单独中断审计进程；

2） 是否无法删除审计记录；

3） 是否无法修改审计记录；

4） 是否无法覆盖审计记录。

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。

#### 7.3.3 审计记录内容

该测评单元包括以下要求：

a） 测评指标：审计记录的内容应包括事件时间、内容、发起者信息、类型、描述和结果。

b） 测评对象：审计记录内容。

c） 测评实施包括以下内容：

1） 审计记录的内容是否包括事件时间；

2） 审计记录的内容是否包括事件内容；

3） 审计记录的内容是否包括事件发起者信息；
4） 审计记录的内容是否包括事件类型；
5） 审计记录的内容是否包括事件描述；
6） 审计记录的内容是否包括事件结果。

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。

#### 7.3.4 活动审计

该测评单元包括以下要求：

a） 测评指标：应保证活动审计具备完整阶段、覆盖全面的审计指标，且审计功能完善。
b） 测评对象：区块链活动审计。
c） 测评实施包括以下内容：
1） 是否对区块链活动的事前、事中、事后三个阶段进行审计；
2） 是否包含查处违规违纪审计、内控制度审计、绩效审计等审计指标；
3） 是否实现区块链服务审计方加入区块链网络作为其中一个节点进行实时审计；
4） 是否允许区块链服务审计方作为区块链网络之外的第三方机构。
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。

#### 7.3.5 审计日志

该测评单元包括以下要求：

a） 测评指标：应保证审计日志内容的完整性。
b） 测评对象：审计日志。
c） 测评实施包括以下内容：
1） 是否保存与审计活动相关的运营环境条件的记录和日志；
2） 是否保存审计员的审计查看动作记录；
3） 是否保存审计过程和结果信息等数据和证据。
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 第四级测评要求

### 8.1 应用系统测评要求

#### 8.1.1 用户身份鉴别

该测评单元包括以下要求：

a） 测评指标：应保证用户身份标识具有唯一性，且用户身份可被安全认证，保证身份鉴别信息的安全性。
b） 测评对象：用户身份认证及鉴别机制。
c） 测评实施包括以下内容：
1） 用户身份标识是否具有唯一性；
2） 是否具备对同一用户采用两种或以上组合的身份认证技术，实现多因子用户身份认证，包

括但不限于密钥、登录码、手机动态码等方式；

3） 是否具备用户身份标识和鉴别信息复杂度检查功能；

4） 是否建立以数字证书为核心的身份认证系统，以安全保密方式实现用户身份鉴别；

5） 远程管理系统时，是否采取必要措施防止鉴别信息在网络传输过程中被泄露；

6） 身份鉴别信息是否要求定期更换。

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 访问控制

该测评单元包括以下要求：

a） 测评指标：应保证区块链系统具备安全、有效的访问控制策略。

b） 测评对象：访问控制策略。

c） 测评实施包括以下内容：

1） 是否按照权限最小化、相互制约原则，为用户分配访问权限；

2） 每个用户交互时是否均检测其访问控制状态；

3） 是否只有授权用户才具备访问秘密数据或敏感数据权限，并且不能越级访问，例如与用户信息或系统自身安全密切相关的状态信息、文件或其他资源、受保护的功能以及与安全相关的配置信息等；

4） 高等级账户是否具备对低等级账户的访问权限进行授予、更改和回收等功能。

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 配置管理

该测评单元包括以下要求：

a） 测评指标：应具备安全配置管理策略。

b） 测评对象：配置信息。

c） 测评实施包括以下内容：

1） 是否提供配置管理功能，对所有配置项进行维护，并唯一标识配置项；

2） 是否提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；

3） 配置信息的变更是否具有相应的申报审批程序；

4） 是否实现配置项或部分配置项配置管理自动化。

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。

#### 8.1.4 备份与故障恢复

该测评单元包括以下要求：

a） 测评指标：应提供完善的系统备份与故障恢复机制。

b） 测评对象：备份与故障恢复机制。

c） 测评实施包括以下内容：

1） 应用系统是否提供数据备份与恢复机制；

2） 是否为系统配置、用户敏感信息等重要数据提供多种备份方式；

3） 是否为用户提供自主选择备份重要信息的功能；

4） 数据恢复后，系统是否进行校验，且可以正常运行；
5） 存储的备份数据是否为密文。

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。

#### 8.1.5 系统异常处理

该测评单元包括以下要求：

a） 测评指标：系统针对异常登录、错误信息等情况应具备异常处理功能。
b） 测评对象：系统异常情况处理机制。
c） 测评实施包括以下内容：
1） 是否提供登录异常处理功能，例如采取结束会话、限制非法登录次数、自动退出或者采用多重认证等手段增强身份验证等措施；
2） 在认证反复出现错误时是否有账户安全警告与锁定功能；
3） 在针对账号信息遗忘等情况是否具备可靠的找回机制。
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 漏洞防护测评要求

#### 8.2.1 注入类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对 SQL 注入、OS 命令注入等注入类漏洞，应具备安全防护措施。
b） 测评对象：漏洞防护方法。
c） 测评实施包括以下内容：
1） 若未使用参数化的应用程序接口，是否使用解释器来避免特殊字符的出现；
2） 是否使用正面或“白名单”中恰当的、规范化的输入验证方法防止注入类攻击；
3） 在区块链项目的 web 端，是否避免动态调用智能合约；
4） 是否采用安全的应用程序接口，避免使用解释器或提供参数化界面的应用程序接口。
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。

#### 8.2.2 跨站类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对跨站脚本、跨站请求伪造等跨站类漏洞，应具备安全防护措施。
b） 测评对象：漏洞防护方法。
c） 测评实施包括以下内容：
1） 查看是否每个链接和表单都提供了不可预测的跨站请求伪造令牌；
2） 是否采用内容安全策略，将不可信数据与动态的浏览器内容区分开，来抵御整个系统的跨站脚本攻击；
3） 应用程序接口是否具备身份验证方案，并且所有凭据、密钥和令牌均已被保护；
4） 是否建立应用程序接口调用的访问控制机制和加密策略，防止跨站类漏洞攻击；
5） 针对能够改变系统状态功能的链接和表格，是否设置独立的检测机制，防止非法攻击。

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。

#### 8.2.3 系统配置类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对安全配置等系统配置类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 开发环境、预发布环境和生产环境是否配置相同，且使用不同的密码；

2） 在各组件之间是否提供一种应用程序框架，可提供有效的组件分离和安全性保障功能；

3） 区块链的联盟链或私有链是否配置加固的、标准的节点，且不允许没有加固的、非标准的服务器成为区块链的节点；

4） 是否设置自动化过程来验证所有环境中配置信息的正确性；

5） 基于开源的区块链项目是否建立淘汰或升级不安全组件的机制。

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。

#### 8.2.4 访问控制类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对功能级访问控制缺失等访问控制类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 是否设置检测攻击机制，例如检测合法用户无法正常输入、异常使用、重复请求等；

2） 是否自动阻止异常请求，禁用或监控不良行为的用户账户；

3） 是否采用特殊的智能合约来判断不正常的用户行为，并且在发现紧急安全问题时，允许智能合约的拥有者停止智能合约的运行，或者运行智能合约自动采取措施停止运行。

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。

#### 8.2.5 数据泄露类漏洞防护

该测评单元包括以下要求：

a） 测评指标：针对敏感数据泄露等数据泄露类漏洞，应具备安全防护措施。

b） 测评对象：漏洞防护方法。

c） 测评实施包括以下内容：

1） 针对没必要存放的、重要的敏感数据，是否设置清除机制；

2） 是否禁止自动完成功能以防止敏感数据收集，禁用包含敏感数据的缓存页面；

3） 在公有链上是否避免存储敏感数据。

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 安全审计测评要求

#### 8.3.1 审计功能

该测评单元包括以下要求：

a） 测评指标：应提供覆盖到每个用户的安全审计功能，对应用的重要安全事件进行审计。

b） 测评对象：审计功能。

c） 测评实施包括以下内容：

1） 是否提供覆盖到每个用户的安全审计功能；

2） 是否对应用的重要安全事件进行审计，且对安全事件进行提醒或告警处理。

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 审计进程及记录

该测评单元包括以下要求：

a） 测评指标：应确保无法单独中断审计进程，无法删除、修改或覆盖审计记录。

b） 测评对象：审计进程及记录。

c） 测评实施包括以下内容：

1） 是否无法单独中断审计进程；

2） 是否无法删除审计记录；

3） 是否无法修改审计记录；

4） 是否无法覆盖审计记录。

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。

### 8.3.3 审计记录内容

该测评单元包括以下要求：

a） 测评指标：审计记录的内容应包括事件时间、内容、发起者信息、类型、描述和结果。

b） 测评对象：审计记录内容。

c） 测评实施包括以下内容：

1） 审计记录的内容是否包括事件时间；

2） 审计记录的内容是否包括事件内容；

3） 审计记录的内容是否包括事件发起者信息；

4） 审计记录的内容是否包括事件类型；

5） 审计记录的内容是否包括事件描述；

6） 审计记录的内容是否包括事件结果。

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。

### 8.3.4 活动审计

该测评单元包括以下要求：

a） 测评指标：应保证活动审计具备完整阶段、覆盖全面的审计指标，且审计功能完善。

b） 测评对象：区块链活动审计。

c） 测评实施包括以下内容：

1） 是否对区块链活动的事前、事中、事后三个阶段进行审计；

2） 是否包含查处违规违纪审计、内控制度审计、绩效审计等审计指标；

3） 是否实现区块链服务审计方加入区块链网络作为其中一个节点进行实时审计；
4） 是否允许区块链服务审计方作为区块链网络之外的第三方机构；
5） 是否按需或定时测评区块链网络中的数据与证据。

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。

#### 8.3.5 审计日志

该测评单元包括以下要求：

a） 测评指标：应保证审计日志内容的完整性。
b） 测评对象：审计日志。
c） 测评实施包括以下内容：
1） 是否保存与审计活动相关的运营环境条件的记录和日志；
2） 是否保存审计员的审计查看动作记录；
3） 是否保存审计过程和结果信息等数据和证据；
4） 是否定期测评审计记录和日志等内容，避免审计信息的泄漏。
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。

## 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 33561—2017 信息安全技术 安全漏洞分类

[2] 刘九良，付章杰，孙星明．区块链安全综述[J]．南京信息工程大学学报(自然科学版)，2019(5)．

[3] 朱岩，甘国华，邓迪,等．区块链关键技术中的安全性研究[J]．信息安全研究，2016(12)．

[4] Wüst K. Security of blockchain technologies[D]. ETH Zürich, 2016.

[5] 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，2019，039(007):1959-1966．

[6] Decker C. On the scalability and security of bitcoin[D]. ETH Zurich, 2016.

[7] 朱岩，宋晓旭，薛显斌,等．基于安全多方计算的区块链智能合约执行系统[J]．密码学报，2019，006(002):246-257．

[8] 陈拥军，孟晓明，庞磊．ASP 的安全漏洞与网络信息安全防护策略研究[J]．计算机应用研究，2004，021(007):75-77．