

# DB43

## 湖 南 省 地 方 标 准

DB43/T 1840—2020

### 信息安全技术 区块链网络安全技术测评要求

Information security technology - Evaluation requirements  
for blockchain network security technology

地方标准信息服务平台

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 物理网络测评要求 ..... 2

    5.2 组网机制测评要求 ..... 3

    5.3 数据传播机制测评要求..... 4

    5.4 数据验证机制测评要求..... 4

    5.5 网络路由机制测评要求..... 5

    5.6 跨链通信测评要求 ..... 5

6 第二级测评要求..... 6

    6.1 物理网络测评要求 ..... 6

    6.2 组网机制测评要求 ..... 7

    6.3 数据传播机制测评要求..... 8

    6.4 数据验证机制测评要求..... 9

    6.5 网络路由机制测评要求..... 9

    6.6 跨链通信测评要求 ..... 10

7 第三级测评要求..... 11

    7.1 物理网络测评要求 ..... 11

    7.2 组网机制测评要求 ..... 12

    7.3 数据传播机制测评要求..... 13

    7.4 数据验证机制测评要求..... 14

    7.5 网络路由机制测评要求..... 14

    7.6 跨链通信测评要求 ..... 15

8 第四级测评要求..... 16

    8.1 物理网络测评要求 ..... 16

    8.2 组网机制测评要求 ..... 17

    8.3 数据传播机制测评要求..... 18

    8.4 数据验证机制测评要求..... 19

|                      |    |
|----------------------|----|
| 8.5 网络路由机制测评要求 ..... | 20 |
| 8.6 跨链通信测评要求 .....   | 20 |
| 9 测评结论 .....         | 21 |
| 9.1 风险分析和评价 .....    | 21 |
| 9.2 等级测评结论 .....     | 21 |
| 参考文献 .....           | 22 |

地方标准信息服务平台

## 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：聂璐璐、梁琪、陈昕、谭林、杨征、李财、梁亮、聂朗、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。

地方标准信息服务平台



# 信息安全技术 区块链网络安全技术测评要求

## 1 范围

本文件规定了区块链网络安全技术测评指标要求。包括第一级、第二级、第三级、第四级区块链网络安全技术测评要求。

本文件适用于测评机构对区块链网络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 5271.18—2008 信息技术 词汇 第18部分：分布式数据处理

GB/T 25069—2010 信息安全技术 术语

GB/T 31491—2015 无线网络访问控制技术规范

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

## 3 术语和定义

GB/T 5271.18.2008、GB/T 25069—2010 界定的下列术语和定义适用于本文件。

### 3.1

**对等网络 peer-to-peer network**

一种仅包含对控制和操作能力等效的节点的计算机网络。

[GB/T 5271.18—2008]

### 3.2

**通信链路 communication link**

网络中两个节点之间的物理通道称为通信链路。通信链路的传输介质主要有双绞线、光纤和微波等。

### 3.3

**结构化网络 structured network**

对网络拓扑结构有着较强组织要求，对等网络中节点的放置受控制，系统中每一个数据文件所放置位置由特定协议决定，具有查询高效和精准的特点。

### 3.4

**帧 frame**

网路中传递的数据包。

### 3.5

**校验码 check code**

校验码通常是一组数字的最后一位，由前面的数字通过某种运算得出，用以检验该组数字的正确性。

### 3.6

**跨链技术 cross-chain communication**

跨链技术是一种将一条链上的数据或信息安全可信地转移到另一条链,并在另一条链上产生预期效果的一种技术。

### 3.7

#### 物理访问控制 **physical access control**

使用物理机制实施访问控制。例如将计算机放在上锁的房间内。

[GB/T 25069—2010]

## 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特定的测评对象,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。单项测评中的每一个具体测评实施要求项(以下简称“测评要求项”)是与安全控制点下面所包括的要求项(测评指标)相对应的。

本标准中每个级别测评要求都包括物理网络测评要求、组网机制测评要求、数据传播机制测评要求、数据验证机制测评要求、网络路由机制测评要求和跨链通信测评要求六部分内容。

### 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 物理网络测评要求

#### 5.1.1 节点设备物理环境

该测评单元包括以下要求:

- a) 测评指标: 节点设备的物理环境应具备安全防护措施。
- b) 测评对象: 节点设备的物理环境。
- c) 测评实施包括以下内容:
  - 1) 对物理设备进行访问控制,机房出入是否安排专人值守或配置电子门禁系统;
  - 2) 是否具备防盗窃和破坏、防雷击和火灾等措施。
- 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 节点运维管理

该测评单元包括以下要求:

- a) 测评指标: 应保证节点设备存放环境的安全性。
- b) 测评对象: 节点设备。
- c) 测评实施包括以下内容:

- 1) 是否指定专员对机房安全、卫生、供配电、温湿和消防等设施进行维护管理;
- 2) 是否将介质存放在安全环境中, 实行存储环境专人管理, 并定期盘点介质的目录与存档。
- 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 节点间通信链路

该测评单元包括以下要求:

- a) 测评指标: 应保证网络节点间链路连接状态正常。
- b) 测评对象: 网络节点。
- c) 测评实施包括以下内容:
  - 1) 源节点在委托要求的预置时间内是否能接收到目标节点转发的检测消息。
- 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。

### 5.1.4 区域边界

该测评单元包括以下要求:

- a) 测评指标: 应保证区域边界的安全性。
- b) 测评对象: 访问控制策略。
- c) 测评实施包括以下内容:
  - 1) 是否提供受控的接口进行通信。
- 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 组网机制测评要求

### 5.2.1 组网扩展性

该测评单元包括以下要求:

- a) 测评指标: 应保证区块链网络中的节点支持动态加入和退出。
- b) 测评对象: 区块链网络节点。
- c) 测评实施包括以下内容:
  - 1) 区块链网络中的节点是否支持动态加入和退出。
- 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。

### 5.2.2 组网安全性

该测评单元包括以下要求:

- a) 测评指标: 应保证区块链网络中的单帧包括帧计数器域。
- b) 测评对象: 网络协议。
- c) 测评实施包括以下内容:
  - 1) 单帧是否包含帧计数器域。
- 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 组网开放性

该测评单元包括以下要求：

- a) 测评指标：应设置区块链网络对外开放的限制措施。
- b) 测评对象：组网机制。
- c) 测评实施包括以下内容：
  - 1) 区块链网络是否能在虚拟逻辑上区分网络内的节点和网络外的节点。
- 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 数据传播机制测评要求

### 5.3.1 数据完整性

该测评单元包括以下要求：

- a) 测评指标：应保证数据在传播的过程中数据完整性不受影响。
- b) 测评对象：数据校验机制。
- c) 测评实施包括以下内容：
  - 1) 节点是否具有鉴别数据完整性的能力。
- 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。

### 5.3.2 数据保密性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络具备数据保密传输处理功能。
- b) 测评对象：数据传输机制。
- c) 测评实施包括以下内容：
  - 1) 区块链网络中数据是否具备端对端互相认证和保密传输能力。
- 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 数据传播时延

该测评单元包括以下要求：

- a) 测评指标：应保证数据的传输时延在规定时间范围内。
- b) 测评对象：数据传输机制；
- c) 测评实施包括以下内容：
  - 1) 在发送节点和接收节点的传输路径上不存在故障节点时，时延是否在 10 秒以内。
- 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。

## 5.4 数据验证机制测评要求

### 5.4.1 数据验证内容

该测评单元包括以下要求：

- a) 测评指标：区块链网络的数据验证应包括数据结构在内的多项内容。

- b) 测评对象：数据验证机制。
- c) 测评实施包括以下内容：
  - 1) 是否包括交易格式的验证；
  - 2) 是否包括交易数据结构的验证。
- 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。

#### 5.4.2 数据验证方式

该测评单元包括以下要求：

- a) 测评指标：区块链网络的数据验证应包括多种验证方式。
- b) 测评对象：数据验证方式。
- c) 测评实施包括以下内容：
  - 1) 是否支持数据校验码验证方式。
- 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。

### 5.5 网络路由机制测评要求

#### 5.5.1 节点发现

该测评单元包括以下要求：

- a) 测评指标：应具有确保在节点加入或离开网络动态感知的路由机制。
- b) 测评对象：节点发现机制。
- c) 测评实施包括以下内容：
  - 1) 是否提供一种安全的初始节点发现方法。
- 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。

#### 5.5.2 消息广播

该测评单元包括以下要求：

- a) 测评指标：区块链网络应具有高效、低时延的消息广播方式。
- b) 测评对象：消息广播机制。
- c) 测评实施包括以下内容：
  - 1) 区块链网络消息广播的方式是否是对等的，每个节点既可以发也可以收。
- 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。

### 5.6 跨链通信测评要求

#### 5.6.1 跨链应用

该测评单元包括以下要求：

- a) 测评指标：跨链应用应具备适宜的构建机制。
- b) 测评对象：跨链应用。
- c) 测评实施包括以下内容：

- 1) 跨链应用构建是否包括跨链应用设计和跨链应用研发。
- 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。

### 5.6.2 跨链技术

该测评单元包括以下要求：

- a) 测评指标：应采用安全的跨链技术。
- b) 测评对象：跨链技术。
- c) 测评实施包括以下内容：
  - 1) 是否采用公证人机制技术；
  - 2) 是否采用哈希锁定技术；
  - 3) 是否采用侧链/中继技术；
  - 4) 是否采用其他安全的跨链技术。
- d) 测评判定：如果以上测评实施内容任意一项为肯定，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。

### 5.6.3 跨链安全

该测评单元包括以下要求：

- a) 测评指标：应保障跨链之后的结果安全可靠。
- b) 测评对象：跨链消息。
- c) 测评实施包括以下内容：
  - 1) 是否提供跨链消息的输入和输出口径；
  - 2) 是否提供跨链消息的真实性证明，例如简单支付验证证明方法。
- 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 第二级测评要求

### 6.1 物理网络测评要求

#### 6.1.1 节点设备物理环境

该测评单元包括以下要求：

- a) 测评指标：节点设备的物理环境应具备安全防护措施。
- b) 测评对象：节点设备的物理环境。
- c) 测评实施包括以下内容：
  - 1) 对物理设备进行访问控制，机房出入是否安排专人值守或配置电子门禁系统；
  - 2) 是否具备防盗窃和破坏、防雷击和火灾等措施；
  - 3) 是否进行合理温湿度控制，设置必要的温湿度调节，使设备机房温湿度的变化在设备运行所允许的范围之内，防止设备受潮老化；
  - 4) 电力供应稳定时，是否在机房供电线路上配置稳压器和过电压防护装置。
- 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 节点运维管理

该测评单元包括以下要求：

- a) 测评指标：针对节点设备，应进行节点运维管理，保证节点设备安全可用。
- b) 测评对象：节点设备。
- c) 测评实施包括以下内容：
  - 1) 是否指定专员对机房安全、卫生、供配电、温湿和消防等设施进行维护管理；
  - 2) 是否将介质存放在安全环境中，实行存储环境专人管理，并定期盘点介质的目录与存档；
  - 3) 是否对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。
- 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。

### 6.1.3 节点间通信链路

该测评单元包括以下要求：

- a) 测评指标：应保证网络节点间链路连接状态正常。
- b) 测评对象：网络节点。
- c) 测评实施包括以下内容：
  - 1) 源节点在委托要求的预置时间内是否能接收到目标节点转发的检测消息；
  - 2) 节点是否能实时输出链路状态连通信息；
  - 3) 若出现异常，是否能及时对出错环节进行判断和反应（如：路由器、交换机、防火墙、物理线路等）。
- 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。

### 6.1.4 区域边界

该测评单元包括以下要求：

- a) 测评指标：应保证区域边界的安全性。
- b) 测评对象：访问控制策略。
- c) 测评实施包括以下内容：
  - 1) 是否提供受控的接口进行通信；
  - 2) 在网络边界设置防火墙和访问控制规则，默认情况下是否允许受控接口拒绝所有通信。
- 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 组网机制测评要求

### 6.2.1 组网扩展性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络中的节点动态加入和退出不会对原有区块链特性造成负面影响。
- b) 测评对象：区块链网络节点。
- c) 测评实施包括以下内容：
  - 1) 区块链网络中的节点是否支持动态加入和退出；

2) 区块链网络中的节点动态变化是否不会对原有区块链特性造成负面影响。

- 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 组网安全性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络中的单帧包括帧计数器域、源地址域、密钥序列号域。
- b) 测评对象：网络协议。
- c) 测评实施包括以下内容：
  - 1) 单帧是否包含帧计数器域；
  - 2) 单帧是否包含源地址域；
  - 3) 单帧是否包含密钥序列号域。
- 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 组网开放性

该测评单元包括以下要求：

- a) 测评指标：应设置区块链网络对外开放的限制措施。
- b) 测评对象：组网机制。
- c) 测评实施包括以下内容：
  - 1) 区块链网络是否能在虚拟逻辑上区分网络内的节点和网络外的节点；
  - 2) 是否只允许对区块链网络内的节点发送数据包。
- 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 数据传播机制测评要求

### 6.3.1 数据完整性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络中的数据在传播的过程中数据完整性不受影响，且具有数据校验协议。
- b) 测评对象：数据传播机制。
- c) 测评实施包括以下内容：
  - 1) 节点是否具有鉴别数据完整性的能力；
  - 2) 网络层数据传播过程是否具有数据校验协议，如校验码。
- 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 数据保密性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络具备数据保密传输处理功能。
- b) 测评对象：数据传输机制。
- c) 测评实施包括以下内容：

- 1) 节点是否具有鉴别数据完整性的能力;
- 2) 网络层数据传播过程是否具有数据校验协议, 如校验码。
- 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 数据传播时延

该测评单元包括以下要求:

- a) 测评指标: 应保证数据的传输时延在规定时间范围内。
- b) 测评对象: 数据传输时延;
- c) 测评实施包括以下内容:
  - 1) 在发送节点和接收节点的传输路径上不存在故障节点时, 时延是否在 10 秒以内;
  - 2) 在发送节点和接收节点间存在故障节点时, 时延是否在 100 秒以内。
- 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 数据验证机制测评要求

### 6.4.1 数据验证内容

该测评单元包括以下要求:

- a) 测评指标: 区块链网络的数据验证应包括数据结构在内的多项内容。
- b) 测评对象: 数据验证机制。
- c) 测评实施包括以下内容:
  - 1) 是否包括交易格式的验证;
  - 2) 是否包括交易数据结构的验证;
  - 3) 是否包括交易格式语法结构的验证。
- 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。

### 6.4.2 数据验证方式

该测评单元包括以下要求:

- a) 测评指标: 区块链网络的数据验证应包括多种验证方式。
- b) 测评对象: 数据验证方式。
- c) 测评实施包括以下内容:
  - 1) 是否支持数据校验码验证方式;
  - 2) 是否支持数字签名验证方式。
- 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。

## 6.5 网络路由机制测评要求

### 6.5.1 节点发现

该测评单元包括以下要求:

- a) 测评指标: 应具有确保在节点加入或离开网络动态感知的路由机制。

- b) 测评对象：节点发现机制。
- c) 测评实施包括以下内容：
  - 1) 是否提供一种安全的初始节点发现方法；
  - 2) 是否提供一种安全的后节点发现方法。
- 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。

#### 6.5.2 消息广播

该测评单元包括以下要求：

- a) 测评指标：区块链网络应具有高效、低时延的消息广播方式。
- b) 测评对象：消息广播机制。
- c) 测评实施包括以下内容：
  - 1) 区块链网络消息广播的方式是否是对等的，每个节点既可以发也可以收；
  - 2) 区块链网络在消息广播的过程中是否能保证每个节点消息一致性。
- 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。

### 6.6 跨链通信测评要求

#### 6.6.1 跨链应用

该测评单元包括以下要求：

- a) 测评指标：跨链应用应具备合适的构建、运行机制。
- b) 测评对象：跨链通信。
- c) 测评实施包括以下内容：
  - 1) 跨链应用构建是否包括跨链应用设计和跨链应用研发；
  - 2) 跨链应用运行是否包括部署、触发、执行、维护、废止。
- 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。

#### 6.6.2 跨链架构

该测评单元包括以下要求：

- a) 测评指标：应采用安全的跨链技术。
- b) 测评对象：跨链技术。
- c) 测评实施包括以下内容：
  - 1) 是否采用公证人机制技术；
  - 2) 是否采用哈希锁定技术；
  - 3) 是否采用侧链/中继技术；
  - 4) 是否采用其他安全的跨链技术。
- d) 测评判定：如果以上测评实施内容任意一项为肯定，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。

#### 6.6.3 跨链安全

该测评单元包括以下要求：

- a) 测评指标：应保障跨链之后的结果安全可信。
- b) 测评对象：跨链消息。
- c) 测评实施包括以下内容：
  - 1) 是否提供跨链消息的输入和输出口径；
  - 2) 是否提供跨链消息的真实性证明，例如简单支付验证证明方法；
  - 3) 消息的有效路由是否构建跨链消息的统一格式，定义消息来源和去处以及消息的内容。
- 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 物理网络测评要求

#### 7.1.1 节点设备物理环境

该测评单元包括以下要求：

- a) 测评指标：节点设备的物理环境应具备安全防护措施。
- b) 测评对象：节点设备的物理环境。
- c) 测评实施包括以下内容：
  - 1) 对物理设备进行访问控制，机房出入是否安排专人值守或配置电子门禁系统；
  - 2) 是否具备防盗窃和破坏、防雷击和火灾等措施；
  - 3) 是否进行合理温湿度控制，设置必要的温湿度调节，使设备机房温湿度的变化在设备运行所允许的范围之内，防止设备受潮老化；
  - 4) 电力供应稳定时，是否在机房供电线路上配置稳压器和过电压防护装置；
  - 5) 是否远离强电磁干扰、强热源等环境。
- 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 节点运维管理

该测评单元包括以下要求：

- a) 测评指标：针对节点设备，应进行节点运维管理，保证节点设备安全可用。
- b) 测评对象：节点设备。
- c) 测评实施包括以下内容：
  - 1) 是否指定专员对机房安全、卫生、供配电、温湿度和消防等设施进行维护管理；
  - 2) 是否将介质存放在安全环境中，实行存储环境专人管理，并定期盘点介质的目录与存档；
  - 3) 是否对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
  - 4) 是否采取必要的措施识别安全漏洞和隐患并及时进行修补和后果评估。
- 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 节点间通信链路

该测评单元包括以下要求：

- a) 测评指标：应保证网络节点间链路连接状态正常。
- b) 测评对象：网络节点。
- c) 测评实施包括以下内容：
  - 1) 源节点在委托要求的预置时间内是否能接收到目标节点转发的检测消息；
  - 2) 节点是否能实时输出链路状态连通信息；
  - 3) 若出现异常，是否能及时对出错环节进行判断和反应（如：路由器、交换机、防火墙、物理线路等）。
- 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。

#### 7.1.4 区域边界

该测评单元包括以下要求：

- a) 测评指标：应保证区域边界的安全性。
- b) 测评对象：访问控制策略。
- c) 测评实施包括以下内容：
  - 1) 是否提供受控的接口进行通信；
  - 2) 在网络边界设置防火墙和访问控制规则，默认情况下是否允许受控接口拒绝所有通信；
  - 3) 是否对源地址、目的地址、源端口、目的端口和协议进行检查来控制数据包的进出。
- 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 组网机制测评要求

#### 7.2.1 组网扩展性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络中的节点动态加入和退出不会对原有区块链特性造成负面影响，且节点增加后会使得区块链系统的安全性得到增强、资源和服务得到扩展。
- b) 测评对象：区块链网络节点。
- c) 测评实施包括以下内容：
  - 1) 区块链网络中的节点是否支持动态加入和退出；
  - 2) 区块链网络中的节点动态变化是否不会对原有区块链特性造成负面影响；
  - 3) 区块链网络中的节点增加后网络系统的安全性是否得到增强、资源和服务是否能得到扩展。
- 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 组网安全性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络中的单帧包括帧计数器域、源地址域、密钥序列号域以及奇偶校验位，保证组网安全性。
- b) 测评对象：网络协议。
- c) 测评实施包括以下内容：

- 1) 单帧是否包含帧计数器域;
- 2) 单帧是否包含源地址域;
- 3) 单帧是否包含密钥序列号域;
- 4) 单帧是否包含奇偶校验位。
- 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 组网开放性

该测评单元包括以下要求:

- a) 测评指标: 应设置区块链网络对外开放的限制措施。
- b) 测评对象: 组网机制。
- c) 测评实施包括以下内容:
  - 1) 区块链网络是否能在虚拟逻辑上区分网络内的节点和网络外的节点;
  - 2) 是否只允许对区块链网络内的节点发送数据包;
  - 3) 加入区块链网络的节点是否可以只分享部分存储资源和服务, 没有分享的存储资源和服务其他节点无权访问。
- 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 数据传播机制测评要求

### 7.3.1 数据完整性

该测评单元包括以下要求:

- a) 测评指标: 应保证数据在传播的过程中数据完整性不受影响, 且具有数据校验协议。
- b) 测评对象: 数据传播机制。
- c) 测评实施包括以下内容:
  - 1) 节点是否具有鉴别数据完整性的能力;
  - 2) 网络层数据传播过程是否具有数据校验协议, 如校验码。
- 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 数据保密性

该测评单元包括以下要求:

- a) 测评指标: 应保证区块链网络具备数据保密传输处理功能。
- b) 测评对象: 数据传输机制。
- c) 测评实施包括以下内容:
  - 1) 区块链网络中数据是否具备端对端互相认证和保密传输能力;
  - 2) 用户安全标准隔离手段是否能保证同一虚拟机环境、网络内环境用户数据以及网络传输对外不可见;
  - 3) 使用密码算法和安全组隔离等手段是否能保证不同节点用户数据互不可见。
- 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 数据传播时延

该测评单元包括以下要求：

- a) 测评指标：应保证数据的传输时延在规定时间范围内。
- b) 测评对象：数据传播时延；
- c) 测评实施包括以下内容：
  - 1) 在发送节点和接收节点的传输路径上不存在故障节点时，时延是否在 10 秒以内；
  - 2) 在发送节点和接收节点间存在故障节点时，时延是否在 100 秒以内。
- 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 数据验证机制测评要求

#### 7.4.1 数据验证内容

该测评单元包括以下要求：

- a) 测评指标：区块链网络的数据验证应包括数据结构在内的多项内容。
- b) 测评对象：数据验证机制。
- c) 测评实施包括以下内容：
  - 1) 是否包括交易格式的验证；
  - 2) 是否包括交易数据结构的验证；
  - 3) 是否包括交易格式语法结构的验证；
  - 4) 是否包括输入输出的验证；
  - 5) 是否包括数字签名验证正确性的验证。
- 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。

#### 7.4.2 数据验证方式

该测评单元包括以下要求：

- a) 测评指标：区块链网络的数据验证应包括多种验证方式。
- b) 测评对象：数据验证方式。
- c) 测评实施包括以下内容：
  - 1) 是否支持数据校验码验证方式；
  - 2) 是否支持数字签名验证方式；
  - 3) 是否支持非对称加密和哈希验证方式。
- 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。

### 7.5 网络路由机制测评要求

#### 7.5.1 节点发现

该测评单元包括以下要求：

- a) 测评指标：应具有确保在节点加入或离开网络动态感知的路由机制。
- b) 测评对象：节点发现机制。
- c) 测评实施包括以下内容：

- 1) 是否提供一种安全的初始节点发现方法;
  - 2) 是否提供一种安全的后节点发现方法;
  - 3) 是否具有黑名单机制。
- 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。

### 7.5.2 消息广播

该测评单元包括以下要求:

- a) 测评指标: 区块链网络应具有高效、低时延的消息广播方式。
- b) 测评对象: 消息广播机制。
- c) 测评实施包括以下内容:
  - 1) 区块链网络消息广播的方式是否是对等的, 每个节点既可以发也可以收;
  - 2) 区块链网络在消息广播的过程中是否能保证每个节点消息一致性。
- 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。

## 7.6 跨链通信测评要求

### 7.6.1 跨链应用

该测评单元包括以下要求:

- a) 测评指标: 跨链应用应具备适宜的构建、运行、评估机制。
- b) 测评对象: 跨链应用。
- c) 测评实施包括以下内容:
  - 1) 跨链应用构建是否包括跨链应用设计和跨链应用研发;
  - 2) 跨链应用运行是否包括部署、触发、执行、维护、废止;
  - 3) 跨链应用评估是否包括但不限于安全审计和质量评价。
- 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。

### 7.6.2 跨链技术

该测评单元包括以下要求:

- a) 测评指标: 应采用安全的跨链技术。
- b) 测评对象: 跨链技术。
- c) 测评实施包括以下内容:
  - 1) 是否采用公证人机制技术;
  - 2) 是否采用哈希锁定技术;
  - 3) 是否采用侧链/中继技术;
  - 4) 是否采用其他安全的跨链技术。
- d) 测评判定: 如果以上测评实施内容任意一项为肯定, 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。

### 7.6.3 跨链安全

该测评单元包括以下要求:

- a) 测评指标：应保障跨链之后的结果安全可信。
- b) 测评对象：跨链消息。
- c) 测评实施包括以下内容：
  - 1) 是否提供跨链消息的输入和输出口径；
  - 2) 是否提供跨链消息的真实性证明，例如简单支付验证证明方法；
  - 3) 消息的有效路由是否构建跨链消息的统一格式，定义消息来源和去处以及消息的内容；
  - 4) 是否提供消息状态的有效性证明。
- 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 物理网络测评要求

#### 8.1.1 节点设备物理环境

该测评单元包括以下要求：

- a) 测评指标：节点设备的物理环境应具备安全防护措施。
- b) 测评对象：节点设备的物理环境。
- c) 测评实施包括以下内容：
  - 1) 对物理设备进行访问控制，机房出入是否安排专人值守或配置电子门禁系统
  - 2) 是否具备防盗窃和破坏、防雷击和火灾等措施；
  - 3) 是否进行合理温湿度控制，设置必要的温湿度调节，使设备机房温湿度的变化在设备运行所允许的范围之内，防止设备受潮老化；
  - 4) 电力供应稳定时，是否在机房供电线路上配置稳压器和过电压防护装置；
  - 5) 是否远离强电磁干扰、强热源等环境；
  - 6) 是否满足 GB/T 22239—2019 中 9.1.1 中规定的内容。
- 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 节点运维管理

该测评单元包括以下要求：

- a) 测评指标：针对节点设备，应进行节点运维管理，保证节点设备安全可用。
- b) 测评对象：节点设备。
- c) 测评实施包括以下内容：
  - 1) 是否指定专员对机房安全、卫生、供配电、温湿和消防等设施进行维护管理；
  - 2) 是否将介质存放在安全环境中，实行存储环境专人管理，并定期盘点介质的目录与存档；
  - 3) 是否对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
  - 4) 是否采取必要的措施识别安全漏洞和隐患并及时进行修补和后果评估；
  - 5) 是否进行木马病毒等恶意攻击行为或文件的检测与查杀。
- 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 节点间通信链路

该测评单元包括以下要求：

- a) 测评指标：应保证网络节点间链路连接状态正常。
- b) 测评对象：网络节点。
- c) 测评实施包括以下内容：
  - 1) 源节点在委托要求的预置时间内是否能接收到目标节点转发的检测消息；
  - 2) 节点是否能实时输出链路状态连通信息；
  - 3) 若出现异常，是否能及时对出错环节进行判断和反应（如：路由器、交换机、防火墙、物理线路等）；
  - 4) 节点之间的丢包率是否能控制在 5% 以下。
- 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 区域边界

该测评单元包括以下要求：

- a) 测评指标：应保证区域边界的安全性。
- b) 测评对象：访问控制策略。
- c) 测评实施包括以下内容：
  - 1) 是否提供受控的接口进行通信；
  - 2) 在网络边界设置防火墙和访问控制规则，默认情况下是否允许受控接口拒绝所有通信；
  - 3) 是否对源地址、目的地址、源端口、目的端口和协议进行检查来控制数据包的进出；
  - 4) 是否基于可信根对计算机设备等进行可信验证。
- 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。

## 8.2 组网机制测评要求

### 8.2.1 组网扩展性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络中的节点动态加入和退出不会对原有区块链特性造成负面影响，且节点增加后会使得区块链系统的安全性得到增强、资源和服务得到扩展。
- b) 测评对象：区块链网络节点。
- c) 测评实施包括以下内容：
  - 1) 区块链网络中的节点是否支持动态加入和退出；
  - 2) 区块链网络中的节点动态变化是否不会对原有区块链特性造成负面影响；
  - 3) 区块链网络中的节点增加后网络系统的安全性是否得到增强，资源和服务是否能得到扩展。
- 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 组网安全性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络中的单帧包括帧计数器域、源地址域、密钥序列号域以及奇偶校

验位，保证组网安全性。

- b) 测评对象：网络协议。
- c) 测评实施包括以下内容：
  - 1) 单帧是否包含帧计数器域；
  - 2) 单帧是否包含源地址域；
  - 3) 单帧是否包含密钥序列号域；
  - 4) 单帧是否包含奇偶校验位。
- 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 组网开放性

该测评单元包括以下要求：

- a) 测评指标：应设置区块链网络对外开放的限制措施。
- b) 测评对象：组网机制。
- c) 测评实施包括以下内容：
  - 1) 区块链网络是否能在虚拟逻辑上区分网络内的节点和网络外的节点；
  - 2) 是否只允许对区块链网络内的节点发送数据包；
  - 3) 加入区块链网络的节点是否可以只分享部分存储资源和服务，没有分享的存储资源和服务其他节点无权访问。
- 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 数据传播机制测评要求

### 8.3.1 数据完整性

该测评单元包括以下要求：

- a) 测评指标：应保证数据在传播的过程中数据完整性不受影响，且具有数据校验协议。
- b) 测评对象：数据传播机制。
- c) 测评实施包括以下内容：
  - 1) 节点是否具有鉴别数据完整性的能力；
  - 2) 网络层数据传播过程是否具有数据校验协议，如校验码。
- 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 数据保密性

该测评单元包括以下要求：

- a) 测评指标：应保证区块链网络具备数据保密传输处理功能。
- b) 测评对象：数据传输机制。
- c) 测评实施包括以下内容：
  - 1) 区块链网络中数据是否具备端对端互相认证和保密传输能力；
  - 2) 用户安全标准隔离手段是否能保证同一虚拟机环境、网络内环境用户数据以及网络传输对外不可见；

- 3) 使用密码算法和安全组隔离等手段是否能保证不同节点用户数据互不可见;
- 4) 在数据传输、网络层访问控制上是否满足国家标准 GB/T 31491—2015 中 6.3 节和 6.6 节规定的内容。
- 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 数据传播时延

该测评单元包括以下要求:

- a) 测评指标: 应保证数据的传输时延在规定时间范围内。
- b) 测评对象: 数据传输时延。
- c) 测评实施包括以下内容:
  - 1) 在发送节点和接收节点的传输路径上不存在故障节点时, 时延是否在 10 秒以内;
  - 2) 在发送节点和接收节点间存在故障节点时, 时延是否在 100 秒以内;
  - 3) 区块链网络全网接收时延是否在 10 分钟以内。
- 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 数据验证机制测评要求

### 8.4.1 数据验证内容

该测评单元包括以下要求:

- a) 测评指标: 区块链网络的数据验证应包括数据结构在内的多项内容。
- b) 测评对象: 数据验证机制。
- c) 测评实施包括以下内容:
  - 1) 是否包括交易格式的验证;
  - 2) 是否包括交易数据结构的验证;
  - 3) 是否包括交易格式语法结构的验证;
  - 4) 是否包括输入输出的验证;
  - 5) 是否包括数字签名验证正确性的验证。
- 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。

### 8.4.2 数据验证方式

该测评单元包括以下要求:

- a) 测评指标: 区块链网络的数据验证应包括多种验证方式。
- b) 测评对象: 数据验证方式。
- c) 测评实施包括以下内容:
  - 1) 是否支持数据校验码验证方式;
  - 2) 是否支持数字签名验证方式;
  - 3) 是否支持非对称加密和哈希验证方式。
- 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。

## 8.5 网络路由机制测评要求

### 8.5.1 节点发现

该测评单元包括以下要求：

- a) 测评指标：应具有确保在节点加入或离开网络动态感知的路由机制。
- b) 测评对象：节点发现机制。
- c) 测评实施包括以下内容：
  - 1) 是否提供一种安全的初始节点发现方法；
  - 2) 是否提供一种安全的后节点发现方法；
  - 3) 是否具有黑名单机制；
  - 4) 是否具有长连接机制。
- 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。

### 8.5.2 消息广播

该测评单元包括以下要求：

- a) 测评指标：区块链网络应具有高效、低时延的消息广播方式。
- b) 测评对象：消息广播。
- c) 测评实施包括以下内容：
  - 1) 区块链网络消息广播的方式是否是对等的，每个节点既可以发也可以收；
  - 2) 区块链网络在消息广播的过程中是否能保证每个节点消息一致性。
- 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。

## 8.6 跨链通信测评要求

### 8.6.1 跨链应用

该测评单元包括以下要求：

- a) 测评指标：跨链应用应具备适宜的构建、运行、评估机制，且跨链实施改进内容合理。
- b) 测评对象：跨链应用。
- c) 测评实施包括以下内容：
  - 1) 跨链应用构建是否包括跨链应用设计和跨链应用研发；
  - 2) 跨链应用运行是否包括部署、触发、执行、维护、废止；
  - 3) 跨链应用评估是否包括但不限于安全审计和质量评价；
  - 4) 跨链实施改进是否包括但不限于对应用构建和运行的改进。
- 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。

### 8.6.2 跨链技术

该测评单元包括以下要求：

- a) 测评指标：应采用安全的跨链技术。
- b) 测评对象：跨链技术。
- c) 测评实施包括以下内容：

- 1) 是否采用公证人机制技术;
  - 2) 是否采用哈希锁定技术;
  - 3) 是否采用侧链/中继技术;
  - 4) 是否采用其他安全的跨链技术。
- d) 测评判定: 如果以上测评实施内容任意一项为肯定, 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。

### 8.6.3 跨链安全

该测评单元包括以下要求:

- a) 测评指标: 应保障跨链之后的结果安全可靠。
- b) 测评对象: 跨链消息。
- c) 测评实施包括以下内容:
  - 1) 是否提供跨链消息的输入和输出口径;
  - 2) 是否提供跨链消息的真实性证明, 例如简单支付验证证明方法;
  - 3) 消息的有效路由是否构建跨链消息的统一格式, 定义消息来源和去处以及消息的内容;
  - 4) 是否提供消息状态的有效性证明;
  - 5) 是否提供跨链执行结果证明。
- 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

等级测评报告应给出等级保护对象的等级测评结论, 确认等级保护对象达到相应等级保护要求的程度。

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] 王坤,李建,谢培泰网络安全协议研究计算机工程与应用,2003-20:168-171.
  - [2] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
  - [3] Halpin H, Piekarska M. Introduction to Security and Privacy on the Blockchain[C]//2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2017: 1-3.
  - [4] 何小东, 易积政, 陈爱斌. 区块链技术的应用进展与发展趋势[J]. 世界科技研究与发展, 2018, 040(006):615-626.
  - [5] YANG W, AGHASIAN E, GARG S, et al. A survey on block chain-based internet service architecture: requirements, challenges, trends, and future[J]. IEEE Access, 2019, 7: 75845-75872.
  - [6] 李芳, LI Fang, 李卓然,等.区块链跨链技术进展研究[J].软件学报, 2019, Vol.30 Issue(6):1649-1660.
  - [7] Taylor P J, Dargahi T, Dehghantanha A, et al. A systematic literature review of blockchain cyber security[J]. Digital Communications and Networks, 2019.
- 

地方标准信息服务平台