

# DB43

## 湖南省地方标准

DB43/T 1838—2020

### 信息安全技术 区块链共识安全技术测评要求

Information security technology - Evaluation requirements  
for blockchain consensus 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 缩略语 ..... 2

5 等级测评概述..... 2

    5.1 等级测评方法..... 2

    5.2 单项测评..... 2

6 第一级测评要求..... 2

    6.1 共识可靠性测评要求..... 2

    6.2 共识终局性测评要求..... 3

    6.3 共识容错性测评要求..... 4

    6.4 共识可审计性测评要求..... 4

    6.5 共识可扩展性测评要求..... 5

7 第二级测评要求..... 6

    7.1 共识可靠性测评要求..... 6

    7.2 共识终局性测评要求..... 6

    7.3 共识容错性测评要求..... 7

    7.4 共识可审计性测评要求..... 8

    7.5 共识可扩展性测评要求..... 9

8 第三级测评要求..... 9

    8.1 共识可靠性测评要求..... 9

    8.2 共识终局性测评要求..... 10

    8.3 共识容错性测评要求..... 11

    8.4 共识可审计性测评要求..... 12

    8.5 共识可扩展性测评要求..... 13

9 第四级测评要求..... 13

    9.1 共识可靠性测评要求..... 13

    9.2 共识终局性测评要求..... 15

    9.3 共识容错性测评要求..... 15

    9.4 共识可审计性测评要求..... 16

    9.5 共识可扩展性测评要求..... 17

10 测评结论 ..... 18

|                    |    |
|--------------------|----|
| 10.1 风险分析和评价 ..... | 18 |
| 10.2 等级测评结论 .....  | 18 |
| 参考文献 .....         | 19 |

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：谭林、陈昕、杨征、梁亮、汪武、聂璐璐、梁琪、李财、聂朗、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。

地方标准信息服务平台



# 信息安全技术 区块链共识安全技术测评要求

## 1 范围

本文件规定了区块链共识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共识安全技术测评要求。

本文件适用于测评机构对区块链共识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

## 3 术语和定义

**GB/T 25069—2010** 界定的下列术语和定义适用于本文件。

### 3.1

#### 区块链 **blockchain**

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

### 3.2

#### 节点 **node**

由区块链网络的参与者操作的分类账本的副本。

### 3.3

#### 共识机制 **consensus mechanism**

指确保系统记账一致性的算法、措施和规则，旨在解决不同节点之间信任的问题。

### 3.4

#### 重放攻击 **replay attack**

一种主动攻击方法，攻击者通过记录通信会话，并在以后某个时刻重放整个会话或者会话的一部分。

**[GB/T 25069—2010]**

### 3.5

#### 终局性 **consistency**

共识一旦确认，就不会被回滚或撤销。

### 3.6

#### 自私挖矿 **selfish mining**

通过扣留区块、拖延公布区块的时间等方式，攻击区块链系统一种攻击方法，其目的是获取额外奖励，并让诚实矿工进行无效计算。

## 4 缩略语

下列缩略语适用于本文件

PoW: 工作量证明 (Proof-of-Work)

PoS: 权益证明 (Proof-of-Stake)

DPoS: 股份授权证明 (Delegated-Proof-of-Stake)

## 5 等级测评概述

### 5.1 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,包括共识攻击防范、共识记录以及共识算法等内容。

本标准中每个级别测评要求都包括共识可靠性测评要求、共识终局性测评要求、共识容错性测评要求、共识可审计性测评要求以及共识可扩展性测评要求五部分内容。

### 5.2 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。

## 6 第一级测评要求

### 6.1 共识可靠性测评要求

#### 6.1.1 共识正确性

该测评单元包括以下要求:

- a) 测评指标: 应保证共识正确且一致性。
- b) 测评对象: 共识过程。
- c) 测评实施包括以下内容:
  - 1) 系统正常运行节点的请求是否能在系统性能所要求的规定时间达成一致的共识;
  - 2) 系统正常运行节点的请求是否能在系统性能所要求的规定时间内达成正确的共识。
- 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,否则不符合本测评单元指标要求。

#### 6.1.2 共识方案

该测评单元包括以下要求:

- a) 测评指标: 应保证共识方案明确应用场景和规模参数。



- b) 测评对象：共识方案。
- c) 测评实施包括以下内容：
  - 1) 共识方案是否能对共识机制的安全适配范围进行规范化校验。
- 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。

### 6.1.3 常见共识攻击防范

该测评单元包括以下要求：

- a) 测评指标：应使用设计合理和安全的共识机制，并能够有效防范常见的共识攻击，如 **51%**攻击等。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 如果采用 **PoS** 或 **DPoS** 算法，是否能防范币龄累计攻击。
- 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。

## 6.2 共识终局性测评要求

### 6.2.1 限定时间内可终局性

该测评单元包括以下要求：

- a) 测评指标：应保证共识算法在可接受的有限时间内具有终局性。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 系统经过一段时间的交互是否可得到结果；
  - 2) 系统交互的结果是否能保证共识一致性。
- 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，否则不符合本测评单元指标要求。

### 6.2.2 链上记录防篡改

该测评单元包括以下要求：

- a) 测评指标：应具备链上记录防篡改特性。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 区块所有内容是否均受到密码技术保护。
- 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。

### 6.2.3 节点独立判断能力

该测评单元包括以下要求：

- a) 测评指标：应保证验证规则满足概然性与统一性。
- b) 测评对象：验证规则。
- c) 测评实施包括以下内容：
  - 1) 共识机制是否包含验证过程。

- 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。

### 6.3 共识容错性测评要求

#### 6.3.1 节点容错性

该测评单元包括以下要求：

- a) 测评指标：共识机制应具备节点容错性。
- b) 测评对象：区块链网络单个节点。
- c) 测评实施包括以下内容：
  - 1) 当连接节点异常时，系统是否仍能正常运行。
- 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。

#### 6.3.2 节点故障

该测评单元包括以下要求：

- a) 测评指标：应保证节点故障对系统影响程度最小。
- b) 测评对象：区块链网络。
- c) 测评实施包括以下内容：
  - 1) 任意不超过理论值的节点数故障时是否不会影响整个系统正常工作；
  - 2) 正常节点对相同的请求是否能做出明确且一致的判断。
- 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，否则不符合本测评单元指标要求。

#### 6.3.3 恶意请求正确响应

该测评单元包括以下要求：

- a) 测评指标：应保证在理论值范围内的恶意节点对系统发出伪造、重复的恶意请求时，系统能够做出正确的响应，保证一致性。
- b) 测评对象：区块链系统。
- c) 测评实施包括以下内容：
  - 1) 理论值范围内的恶意节点对系统发出伪造请求时，系统是否能够做出正确且一致的响应；
  - 2) 理论值范围内的恶意节点对系统发出重复请求时，系统是否能够做出正确且一致的响应。
- 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，否则不符合本测评单元指标要求。

### 6.4 共识可审计性测评要求

#### 6.4.1 共识记录内容

该测评单元包括以下要求：

- a) 测评指标：应保证共识记录内容的完整性。
- b) 测评对象：共识记录内容。
- c) 测评实施包括以下内容：
  - 1) 共识记录的内容是否包括事件时间；

- 2) 共识记录的内容是否包括事件内容;
- 3) 共识记录的内容是否包括事件发起者信息;
- 4) 共识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, 否则不符合本测评单元指标要求。

#### 6.4.2 共识记录管理

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共识进程, 无法删除、修改或覆盖共识记录。
- b) 测评对象: 共识记录管理。
- c) 测评实施包括以下内容:
  - 1) 是否无法修改共识记录。
- 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。

#### 6.4.3 共识过程审计

该测评单元包括以下要求:

- a) 测评指标: 应保证单次共识过程可审计、可监管且不可被篡改。
- b) 测评对象: 共识历史。
- c) 测评实施包括以下内容:
  - 1) 单次共识过程是否可审计、可监管且不可被篡改。
- 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。

#### 6.4.4 共识历史审计

该测评单元包括以下要求:

- a) 测评指标: 应保证系统运行的整个共识历史都应可审计、可监管且不可被篡改。
- b) 测评对象: 共识历史。
- c) 测评实施包括以下内容:
  - 1) 系统运行的整个共识历史是否可审计、可监管且不可被篡改。
- 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。

### 6.5 共识可扩展性测评要求

#### 6.5.1 共识节点

该测评单元包括以下要求:

- a) 测评指标: 应支持共识节点可扩展。
- b) 测评对象: 区块链网络。
- c) 测评实施包括以下内容:
  - 1) 任意不超过理论值的节点数退出时是否不会影响整个系统正常工作。
- 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。

## 7 第二级测评要求

### 7.1 共识可靠性测评要求

#### 7.1.1 共识正确性

该测评单元包括以下要求：

- a) 测评指标：应保证共识正确且一致性。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 系统正常运行节点的请求是否能在系统性能所要求的规定时间达成一致的共识；
  - 2) 系统正常运行节点的请求是否能在系统性能所要求的规定时间内达成正确的共识；
  - 3) 系统正常运行节点的请求是否能输出正确结果。
- 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，否则不符合本测评单元指标要求。

#### 7.1.2 共识方案

该测评单元包括以下要求：

- a) 测评指标：应保证共识方案明确应用场景和规模参数。
- b) 测评对象：共识方案。
- c) 测评实施包括以下内容：
  - 1) 共识方案是否能对共识机制的安全适配范围进行规范化校验；
  - 2) 共识方案是否明确应用场景和规模参数。
- 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 常见共识攻击防范

该测评单元包括以下要求：

- a) 测评指标：应使用设计合理和安全的共识机制，并能够有效防范常见的共识攻击，如 **51%**攻击等。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 如果采用 **PoS** 或 **DPoS** 算法，是否能防范币龄累计攻击；
  - 2) 如果采用 **PoW** 算法，是否能防范双花攻击。
- 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，否则不符合本测评单元指标要求。

### 7.2 共识终局性测评要求

#### 7.2.1 限定时间内可终局性

该测评单元包括以下要求：

- a) 测评指标：应保证共识算法在可接受的有限时间内具有终局性。
- b) 测评对象：共识过程。

- c) 测评实施包括以下内容：
  - 1) 系统经过一段时间的交互是否可得到结果；
  - 2) 系统交互的结果是否能保证共识一致性。
- 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，否则不符合本测评单元指标要求。

### 7.2.2 链上记录防篡改要求

该测评单元包括以下要求：

- a) 测评指标：应具备链上记录防篡改特性。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 区块所有内容是否均受到密码技术保护；
  - 2) 系统是否能够防止链上交易回滚。
- 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 节点独立判断能力

该测评单元包括以下要求：

- a) 测评指标：应保证验证规则满足概然性与统一性。
- b) 测评对象：验证规则。
- c) 测评实施包括以下内容：
  - 1) 共识机制是否包含验证过程。
- 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，否则不符合本测评单元指标要求。

## 7.3 共识容错性测评要求

### 7.3.1 节点容错性

该测评单元包括以下要求：

- a) 测评指标：共识机制应具备节点容错性。
- b) 测评对象：区块链网络单个节点。
- c) 测评实施包括以下内容：
  - 1) 当连接节点异常时，系统是否仍能正常运行；
  - 2) 是否设定系统正常运行的最大异常节点数。
- 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 节点故障

该测评单元包括以下要求：

- a) 测评指标：应保证节点故障对系统影响程度最小。
- b) 测评对象：区块链网络。
- c) 测评实施包括以下内容：
  - 1) 任意不超过理论值的节点数故障时是否不会影响整个系统正常工作；

2) 正常节点对相同的请求是否能做出明确且一致的判断。

- 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，否则不符合本测评单元指标要求。

### 7.3.3 恶意请求正确响应要求

该测评单元包括以下要求：

- a) 测评指标：应保证在理论值范围内的恶意节点对系统发出伪造、重复的恶意请求时，系统能够做出正确的响应，保证一致性。
- b) 测评对象：区块链系统。
- c) 测评实施包括以下内容：
  - 1) 理论值范围内的恶意节点对系统发出伪造请求时，系统是否能够做出正确且一致的响应；
  - 2) 理论值范围内的恶意节点对系统发出重复请求时，系统是否能够做出正确且一致的响应。
- 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，否则不符合本测评单元指标要求。

## 7.4 共识可审计性测评要求

### 7.4.1 共识记录内容

该测评单元包括以下要求：

- a) 测评指标：应保证共识记录内容的完整性。
- b) 测评对象：共识记录内容。
- c) 测评实施包括以下内容：
  - 1) 共识记录的内容是否包括事件时间；
  - 2) 共识记录的内容是否包括事件内容；
  - 3) 共识记录的内容是否包括事件发起者信息；
  - 4) 共识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，否则不符合本测评单元指标要求。

### 7.4.2 共识记录管理

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共识进程，无法删除、修改或覆盖共识记录。
- b) 测评对象：共识记录管理。
- c) 测评实施包括以下内容：
  - 1) 是否无法修改共识记录；
  - 2) 是否无法单独中断共识进程。
- 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 共识过程审计

该测评单元包括以下要求：

- a) 测评指标：应保证单次共识过程可审计、可监管且不可被篡改。
- b) 测评对象：共识历史。



c) 测评实施包括以下内容：

1) 单次共识过程是否可审计、可监管且不可被篡改。

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。

#### 7.4.4 共识历史审计

该测评单元包括以下要求：

a) 测评指标：应保证系统运行的整个共识历史都应可审计、可监管且不可被篡改。

b) 测评对象：共识历史。

c) 测评实施包括以下内容：

1) 系统运行的整个共识历史是否可审计、可监管且不可被篡改。

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。

### 7.5 共识可扩展性测评要求

#### 7.5.1 共识节点

该测评单元包括以下要求：

a) 测评指标：应支持共识节点可扩展。

b) 测评对象：区块链网络。

c) 测评实施包括以下内容：

1) 任意不超过理论值的节点数退出时是否不会影响整个系统正常工作；

2) 节点数增加是否不会影响整个系统正常工作。

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 第三级测评要求

### 8.1 共识可靠性测评要求

#### 8.1.1 共识正确性

该测评单元包括以下要求：

a) 测评指标：应保证共识正确且一致性。

b) 测评对象：共识过程。

c) 测评实施包括以下内容：

1) 系统正常运行节点的请求是否能在系统性能所要求的规定时间达成一致的共识；

2) 系统正常运行节点的请求是否能在系统性能所要求的规定时间内达成正确的共识；

3) 系统正常运行节点的请求是否能输出正确结果。

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，否则不符合本测评单元指标要求。

#### 8.1.2 共识方案

该测评单元包括以下要求：

- a) 测评指标：应保证共识方案明确应用场景和规模参数。
- b) 测评对象：共识方案。
- c) 测评实施包括以下内容：
  - 1) 共识方案是否能对机制的安全适配范围进行规范化的校验；
  - 2) 共识方案是否伴随清晰的应用场景和规模参数。
- 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 常见共识攻击防范

该测评单元包括以下要求：

- a) 测评指标：应使用设计合理和安全的共识机制，并能够有效防范常见的共识攻击，如 **51%**攻击等。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 如果采用 **PoS** 或 **DPoS** 算法，是否能防范币龄累计攻击；
  - 2) 如果采用 **PoW** 算法，是否能防范双花攻击；
  - 3) 如果采用确定性共识算法，是否能防范确定性算法重放攻击；
  - 4) 如果采用确定性共识算法，是否能防范确定性算法权利压迫攻击。
- 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，否则不符合本测评单元指标要求。

### 8.1.4 算法参数调整

该测评单元包括以下要求：

- a) 测评指标：应提供调整算法参数功能。
- b) 测评对象：包含共识算法的共识层。
- c) 测评实施包括以下内容：
  - 1) 是否可以调整算法中网络规模的参数；
  - 2) 是否可以调整算法中参与方数量的参数；
  - 3) 是否可以调整算法中交易吞吐量需求的参数。
- 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 共识终局性测评要求

### 8.2.1 限定时间内可终局性

该测评单元包括以下要求：

- a) 测评指标：应保证共识算法在可接受的有限时间内具有终局性。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 系统经过一段时间的交互是否可得到结果；
  - 2) 系统交互的结果是否能保证共识一致性。
- 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，否则不符合本测评



单元指标要求。

### 8.2.2 链上记录防篡改

该测评单元包括以下要求：

- a) 测评指标：应具备链上记录防篡改特性。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 区块所有内容是否均受到密码技术保护；
  - 2) 系统是否能够防止链上交易回滚；
  - 3) 链上记录是否能通过有限确认块数达到记录稳定状态。
- 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。

### 8.2.3 节点独立判断能力

该测评单元包括以下要求：

- a) 测评指标：应保证验证规则满足概然性与统一性。
- b) 测评对象：验证规则。
- c) 测评实施包括以下内容：
  - 1) 共识机制是否包含验证过程；
  - 2) 验证规则中每一参与节点是否具有独立判断能力。
- 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，否则不符合本测评单元指标要求。

## 8.3 共识容错性测评要求

### 8.3.1 节点容错性

该测评单元包括以下要求：

- a) 测评指标：共识机制应具备节点容错性。
- b) 测评对象：区块链网络单个节点。
- c) 测评实施包括以下内容：
  - 1) 当连接节点异常时，系统是否仍能正常运行；
  - 2) 是否设定系统正常运行的最大异常节点数；
  - 3) 当连接节点缓慢时，系统是否仍能正常运行。
- 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。

### 8.3.2 节点故障

该测评单元包括以下要求：

- a) 测评指标：应保证节点故障对系统影响程度最小。
- b) 测评对象：区块链网络。
- c) 测评实施包括以下内容：
  - 1) 任意不超过理论值的节点数故障时是否不会影响整个系统正常工作；
  - 2) 正常节点对相同的请求是否能做出明确且一致的判断。

- 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，否则不符合本测评单元指标要求。

### 8.3.3 恶意请求正确响应

该测评单元包括以下要求：

- a) 测评指标：应保证在理论值范围内的恶意节点对系统发出伪造、重复的恶意请求时，系统能够做出正确的响应，保证一致性。
- b) 测评对象：区块链系统。
- c) 测评实施包括以下内容：
  - 1) 理论值范围内的恶意节点对系统发出伪造请求时，系统是否能够做出正确且一致的响应；
  - 2) 理论值范围内的恶意节点对系统发出重复请求时，系统是否能够做出正确且一致的响应。
- 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，否则不符合本测评单元指标要求。

## 8.4 共识可审计性测评要求

### 8.4.1 共识记录内容

该测评单元包括以下要求：

- a) 测评指标：应保证共识记录内容的完整性。
- b) 测评对象：共识记录内容。
- c) 测评实施包括以下内容：
  - 1) 共识记录的内容是否包括事件时间；
  - 2) 共识记录的内容是否包括事件内容；
  - 3) 共识记录的内容是否包括事件发起者信息；
  - 4) 共识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，否则不符合本测评单元指标要求。

### 8.4.2 共识记录管理

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共识进程，无法删除、修改或覆盖共识记录。
- b) 测评对象：共识记录管理。
- c) 测评实施包括以下内容：
  - 1) 是否无法修改共识记录；
  - 2) 是否无法单独中断共识进程；
  - 3) 是否无法删除共识记录。
- 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。

### 8.4.3 共识过程审计

该测评单元包括以下要求：

- a) 测评指标：应保证单次共识过程可审计、可监管且不可被篡改。
- b) 测评对象：共识历史。

c) 测评实施包括以下内容：

1) 单次共识过程是否可审计、可监管且不可被篡改。

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。

#### 8.4.4 共识历史审计

该测评单元包括以下要求：

a) 测评指标：应保证系统运行的整个共识历史都应可审计、可监管且不可被篡改。

b) 测评对象：共识历史。

c) 测评实施包括以下内容：

1) 系统运行的整个共识历史是否可审计、可监管且不可被篡改。

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。

### 8.5 共识可扩展性测评要求

#### 8.5.1 共识节点

该测评单元包括以下要求：

a) 测评指标：应支持共识节点可扩展。

b) 测评对象：区块链网络。

c) 测评实施包括以下内容：

1) 任意不超过理论值的节点数退出时是否不会影响整个系统正常工作；

2) 节点数增加是否不会影响整个系统正常工作。

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 共识算法

该测评单元包括以下要求：

a) 测评指标：应支持多种共识算法并实现共识算法可切换。

b) 测评对象：包含共识算法的共识层。

c) 测评实施包括以下内容：

1) 是否支持多种共识算法。

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。

## 9 第四级测评要求

### 9.1 共识可靠性测评要求

#### 9.1.1 共识正确性

该测评单元包括以下要求：

a) 测评指标：应保证共识正确且一致性。

b) 测评对象：共识过程。

- c) 测评实施包括以下内容：
  - 1) 系统正常运行节点的请求是否能在系统性能所要求的规定时间达成一致的共识；
  - 2) 系统正常运行节点的请求是否能在系统性能所要求的规定时间内达成正确的共识；
  - 3) 系统正常运行节点的请求是否能输出正确结果。
- 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，否则不符合本测评单元指标要求。

### 9.1.2 共识方案

该测评单元包括以下要求：

- a) 测评指标：应保证共识方案明确应用场景和规模参数。
- b) 测评对象：共识方案。
- c) 测评实施包括以下内容：
  - 1) 共识方案是否能对共识机制的安全适配范围进行规范化校验；
  - 2) 共识方案是否明确应用场景和规模参数。
- 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。

### 9.1.3 常见共识攻击防范

该测评单元包括以下要求：

- a) 测评指标：应使用设计合理和安全的共识机制，并能够有效防范常见的共识攻击，如 **51%**攻击等。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 如果采用 **PoS** 或 **DPoS** 算法，是否能防范币龄累计攻击；
  - 2) 如果采用 **PoW** 算法，是否能防范双花攻击；
  - 3) 如果采用确定性共识算法，是否能防范确定性算法重放攻击；
  - 4) 如果采用确定性共识算法，是否能防范确定性算法权利压迫攻击；
  - 5) 如果采用 **PoW** 算法，是否能防范 **51%**攻击；
  - 6) 如果采用 **PoW** 算法，是否能防范自私挖矿。
- 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，否则不符合本测评单元指标要求。

### 9.1.4 算法参数调整

该测评单元包括以下要求：

- a) 测评指标：应提供调整算法参数功能。
- b) 测评对象：包含共识算法的共识层。
- c) 测评实施包括以下内容：
  - 1) 是否可以调整算法中网络规模的参数；
  - 2) 是否可以调整算法中参与方数量的参数；
  - 3) 是否可以调整算法中交易吞吐量需求的参数。
- 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。

## 9.2 共识终局性测评要求

### 9.2.1 限定时间内可终局性

该测评单元包括以下要求：

- a) 测评指标：应保证共识算法在可接受的有限时间内具有终局性。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 系统经过一段时间的交互是否可得到结果；
  - 2) 系统交互的结果是否能保证共识一致性。
- 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，否则不符合本测评单元指标要求。

### 9.2.2 链上记录防篡改

该测评单元包括以下要求：

- a) 测评指标：应具备链上记录防篡改特性。
- b) 测评对象：共识过程。
- c) 测评实施包括以下内容：
  - 1) 区块所有内容是否均受到密码技术保护；
  - 2) 系统是否能够防止链上交易回滚；
  - 3) 链上记录是否能通过有限确认块数达到记录稳定状态。
- 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。

### 9.2.3 节点独立判断能力

该测评单元包括以下要求：

- a) 测评指标：应保证验证规则满足概然性与统一性。
- b) 测评对象：验证规则。
- c) 测评实施包括以下内容：
  - 1) 共识机制是否包含验证过程；
  - 2) 验证规则中每一参与节点是否具有独立判断能力。
- 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，否则不符合本测评单元指标要求。

## 9.3 共识容错性测评要求

### 9.3.1 节点容错性

该测评单元包括以下要求：

- a) 测评指标：共识机制应具备节点容错性。
- b) 测评对象：区块链网络单个节点。
- c) 测评实施包括以下内容：
  - 1) 当连接节点异常时，系统是否仍能正常运行；
  - 2) 是否设定系统正常运行的最大异常节点数；
  - 3) 当连接节点缓慢时，系统是否仍能正常运行；

4) 当连接节点异常时,系统是否能排除异常节点。

- 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。

### 9.3.2 节点故障

该测评单元包括以下要求:

- a) 测评指标:应保证节点故障对系统影响程度最小。
- b) 测评对象:区块链网络。
- c) 测评实施包括以下内容:
  - 1) 任意不超过理论值的节点数故障时是否不会影响整个系统正常工作;
  - 2) 正常节点对相同的请求是否能做出明确且一致的判断。
- 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,否则不符合本测评单元指标要求。

### 9.3.3 恶意请求正确响应

该测评单元包括以下要求:

- a) 测评指标:应保证在理论值范围内的恶意节点对系统发出伪造、重复的恶意请求时,系统能够做出正确的响应,保证一致性。
- b) 测评对象:区块链系统。
- c) 测评实施包括以下内容:
  - 1) 理论值范围内的恶意节点对系统发出伪造请求时,系统是否能够做出正确且一致的响应;
  - 2) 理论值范围内的恶意节点对系统发出重复请求时,系统是否能够做出正确且一致的响应。
- 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,否则不符合本测评单元指标要求。

## 9.4 共识可审计性测评要求

### 9.4.1 共识记录内容

该测评单元包括以下要求:

- a) 测评指标:应保证共识记录内容的完整性。
- b) 测评对象:共识记录内容。
- c) 测评实施包括以下内容:
  - 1) 共识记录的内容是否包括事件时间;
  - 2) 共识记录的内容是否包括事件内容;
  - 3) 共识记录的内容是否包括事件发起者信息;
  - 4) 共识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,否则不符合本测评单元指标要求。

### 9.4.2 共识记录管理

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共识进程,无法删除、修改或覆盖共识记录。
- b) 测评对象:共识记录管理。



- c) 测评实施包括以下内容：
  - 1) 是否无法修改共识记录；
  - 2) 是否无法单独中断共识进程；
  - 3) 是否无法删除共识记录；
  - 4) 是否无法覆盖共识记录。
- 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。

#### 9.4.3 共识过程审计

该测评单元包括以下要求：

- a) 测评指标：应保证单次共识过程可审计、可监管且不可被篡改。
- b) 测评对象：共识历史。
- c) 测评实施包括以下内容：
  - 1) 单次共识过程是否可审计、可监管且不可被篡改。
- 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。

#### 9.4.4 共识历史审计

该测评单元包括以下要求：

- a) 测评指标：应保证系统运行的整个共识历史都应可审计、可监管且不可被篡改。
- b) 测评对象：共识历史。
- c) 测评实施包括以下内容：
  - 1) 系统运行的整个共识历史是否可审计、可监管且不可被篡改。
- 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。

### 9.5 共识可扩展性测评要求

#### 9.5.1 共识节点

该测评单元包括以下要求：

- a) 测评指标：应支持共识节点可扩展。
- b) 测评对象：区块链网络。
- c) 测评实施包括以下内容：
  - 1) 任意不超过理论值的节点数退出时是否不会影响整个系统正常工作；
  - 2) 节点数增加是否不会影响整个系统正常工作。
- 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。

#### 9.5.2 共识算法

该测评单元包括以下要求：

- a) 测评指标：应支持多种共识算法并实现共识算法可切换。
- b) 测评对象：包含共识算法的共识层。
- c) 测评实施包括以下内容：

- 1) 是否支持多种共识算法;
- 2) 是否能根据需求切换并选择共识算法。
- 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。

## 10 测评结论

### 10.1 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。

### 10.2 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。

地方标准信息服务平台



## 参 考 文 献

- [1] 刘懿中, 刘建伟, 张宗洋, 等. 区块链共识机制研究综述[J]. 密码学报, 2019, 6(4).
- [2] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 002(011):P.11-20.
- [3] 周邺飞. 区块链核心技术演进之路——共识机制演进(1)[J]. 计算机教育, 2017(4).
- [4] 唐长兵, 杨珍, 郑忠龙, 等. PoW 共识算法中的博弈困境分析与优化[J]. 自动化学报, 2017(9).
- [5] King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper, August, 2012, 19.
- [6] 任佩, 刘润一. 区块链技术中共识机制的安全分析[J]. 2019 中国网络安全等级保护和关键信息基础设施保护大会论文集, 2019.
- [7] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm[C]//2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14). 2014: 305-319.
- [8] Nguyen G T, Kim K. A Survey about Consensus Algorithms Used in Blockchain[J]. Journal of Information processing systems, 2018, 14(1).
- [9] 斯雪明, 徐蜜雪, 苑超. 区块链安全研究综述[J]. 密码学报, 2018, 5(05):8-19.
- 

地方标准信息服务平台