

# 中华人民共和国国家标准

GB/T 43575—2023

## 区块链和分布式记账技术 系统测试规范

Blockchain and distributed ledger technology—  
System testing specification

国家标准全文公开系统专用，此文本仅供个人学习、研究之用，  
未经授权，禁止复制、发行、汇编、翻译或网络传播等，侵权必究。  
全国标准信息公共服务平台：<https://std.samr.gov.cn>



2023-12-28 发布

2024-04-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会



目 次

前言 ..... I

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 测试原则和类别 ..... 2

    5.1 原则 ..... 2

    5.2 类别 ..... 3

6 测试要求 ..... 3

    6.1 功能测试要求 ..... 3

    6.2 性能测试要求 ..... 4

    6.3 安全测试要求 ..... 5

    6.4 可靠性测试要求 ..... 6

7 测试程序 ..... 6

    7.1 概述 ..... 6

    7.2 需求分析 ..... 7

    7.3 策划设计 ..... 7

    7.4 测试执行 ..... 8

    7.5 总结改进 ..... 8

    7.6 测试管理 ..... 8

8 测试方法 ..... 9

    8.1 功能测试 ..... 9

    8.2 性能测试 ..... 9

    8.3 安全测试 ..... 9

    8.4 可靠性测试 ..... 10

附录 A（规范性） 区块链系统功能测试和性能测试项列表 ..... 11

    A.1 功能测试 ..... 11

    A.2 性能测试 ..... 14

参考文献 ..... 15

# 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国区块链和分布式记账技术标准化技术委员会(SAC/TC 590)归口。

本文件起草单位：中国电子技术标准化研究院、上海万向区块链股份公司、杭州趣链科技有限公司、浙江大学、京东科技信息技术有限公司、四川长虹电器股份有限公司、厦门安妮股份有限公司、深圳市腾讯计算机系统有限公司、蚂蚁科技集团股份有限公司、众安信息技术服务有限公司、上海分布信息科技有限公司、联通数字科技有限公司、江苏恒为信息科技有限公司、永旗控股(北京)有限公司、浙商银行股份有限公司、工银科技有限公司、南京鑫智链科技信息有限公司、上海树图区块链研究院、湖南天河国云科技有限公司、中国民航信息网络股份有限公司、工业和信息化部电子第五研究所、国家工业信息安全发展研究中心、复旦大学、北京微芯区块链与边缘计算研究院、广州南方投资集团有限公司、北京软件产品质量检测检验中心、北京中电众维软件评测中心、北京大数据先进技术研究院、华为技术有限公司、华为云计算技术有限公司、上海零数众合信息科技有限公司、腾讯云计算(北京)有限责任公司、云南财经大学、香港理工大学、大连工业大学艺术与信息工程学院、中国电子科技网络信息安全有限公司、上海阵方科技有限公司、敏于行(北京)科技有限公司、神州数码信息服务股份有限公司、深圳博思互联科技有限公司、达闼机器人股份有限公司、上海奥若拉信息科技集团有限公司、成都质数斯达克科技有限公司、国家应用软件产品质量检验检测中心。

本文件主要起草人：李鸣、张栋、刘亭杉、周平、于秀明、杜宇、谢怡君、昌文婷、王晨辉、郝玉琨、陈晓丰、王威、冯承勇、靳涵、杨征、劳卫伦、张敬之、赵伟、贾超、张春光、笪鸿飞、王思宁、李努锲、欧昀、李克鹏、王荆楠、陶立春、王义、王海龙、安红章、李斌、相里朋、阚海斌、蔡亮、包小敏、唐博、郝汉、张小军、王保春、梁军、彭晋、王琰然、王文呈、张何东、崔春生、董进、唐琳、兰春嘉、孙林、赵玉霞、杨珍、孙琳、武杨、李力、龚自洪、刘天成、王子博、宋文鹏、谢辉、杨国正、王绍刚、周海京、晏海水、陶立春、余益民、曹建农、刘齐军、余姗姗、杨巨森、李哲、张亮亮、李伟、邱炜伟、邓柯、李卫、李孰侨、佟伟、杨文锋、张子怡、曲强、廉贵清、毛超逸、刘冕宸、周子茗、张雁、胡怀勇、翟耀超、张晓蒙。



# 区块链和分布式记账技术 系统测试规范

## 1 范围

本文件确立了区块链系统的测试原则,规定了功能、性能、安全和可靠性测试要求,描述了相应测试方法。

本文件适用于:为第三方测评机构或其他相关机构开展区块链系统测试提供参考;为区块链系统建设方提供内部测试依据;为区块链系统使用方开展系统选型和验收提供依据;为行业主管部门的监管工作提供技术支撑。

## 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 11457—2006 信息技术 软件工程术语
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 25069—2022 信息安全技术 术语
- GB/T 29835.1—2013 系统与软件效率 第1部分:指标体系

## 3 术语和定义



GB/T 11457—2006、GB/T 25069—2022 界定的以及下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。  
[来源:GB/T 5271.18—2008,2.18.04.05,有修改]

### 3.2

**加密 encipherment; encryption**  
对数据进行密码变换以产生密文的过程。  
[来源:GB/T 25069—2022,3.278]

### 3.3

**功能组件 functional component**  
参与活动所需的,可实现的一个功能性基本构件块。  
[来源:GB/T 32399—2015,3.2.1,有修改]

### 3.4

**数字签名 digital signature**  
附加在数据单元上的数据,或是对数据单元做密码变换,这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性,达到保护数据,防止被人(例如接收者)伪造的目的。

[来源:GB/T 25069—2022,3.576]

3.5

**摘要算法**    **digest algorithm**

**摘要函数**    **digest function**

**Hash 函数**    **hash function**

通过将任意长度的消息输入变成固定长度的短消息输出来保障数据的完整性。

3.6

**智能合约**    **smart contract**

存储在分布式记账技术系统中的计算机程序,该程序的任何执行结果都记录在分布式账本中。

[来源:GB/T 43572—2023,3.72]

3.7

**功能测试**    **function test**

忽略系统或部件的内部机制,只集中于响应所选择的输入和执行条件产生的一种测试。

[来源:GB/T 11457—2006,2.669,有修改]

3.8

**性能测试**    **performance test**

评价系统或部件与规定的额性能需求的依从性的测试行为。

[来源:GB/T 11457—2006,2.1135]

3.9

**安全测试**    **security test**

测试对象、相关数据和信息受保护程度,未经允许的个人和系统无法使用、读取和修改。

[来源:ISO/IEC/IEEE 29119-1:2022,3.74]

3.10

**可靠性**    **reliability**

在规定时间间隔内和规定条件下,系统或部件执行所需求功能的能力。

[来源:GB/T 11457—2006,2.1334]

4 缩略语

下列缩略语适用于本文件。

API: 应用程序接口(Application Programming Interface)

CPU: 中央处理器(Central Processing Unit)

DDoS: 分布式拒绝服务攻击(Distributed Denial of Service)

DNS: 域名系统(Domain Name Server)

P2P: 点对点(Peer to Peer)

SM2: 国密算法 SM2(SM2 Cryptographic Algorithm)

SM3: 国密算法 SM3(SM3 Cryptographic Algorithm)

SM4: 国密算法 SM4(SM4 Cryptographic Algorithm)

5 测试原则和类别

5.1 原则

在区块链系统测试过程中,遵循下列原则:



- a) 客观性原则：确切了解区块链系统的技术和业务逻辑，明确测试范围和边界，规避测试风险和约束，客观、公正、独立的记录和总结被测区块链系统的真实情况；
- b) 保密性原则：对测试过程中获知的客户系统、源代码和相关技术文档以及数据保密，不利用这些信息进行任何非授权的活动，测试报告不扩散给未经授权的第三方；
- c) 规范性原则：测试以本文件为依据，由具有专业资格的测试人员依照规范的操作流程实施。测试人员应按测试方案的要求，完成测试环境配置、测试代码部署等准备工作，并详细记录操作过程和结果，提供完整的测试报告。

5.2 类别

区块链系统测试要求类别应包含功能测试、性能测试、安全测试和可靠性测试。

6 测试要求

6.1 功能测试要求

6.1.1 通则

功能测试应覆盖区块链系统功能组件中的用户层、服务接口层、核心功能层、基础设施层等功能组件，见图 1，具体测试项按附录 A 中表 A.1 执行。

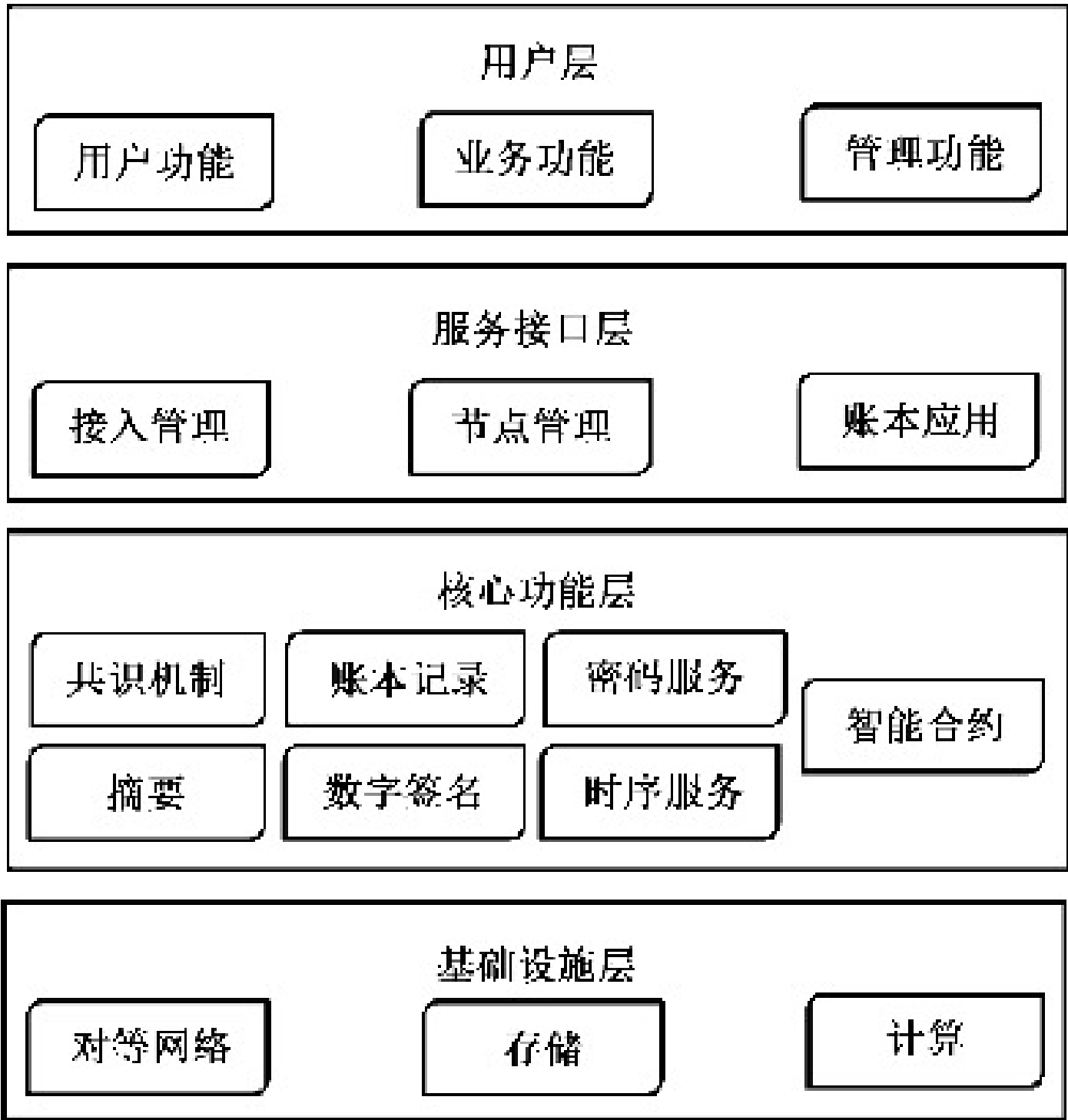


图 1 区块链功能组件

6.1.2 用户层

用户层测试要求应包含但不限于：

- a) 具备用户界面，可采用命令行、图形交互或 API 等形式；
- b) 具备用户事务提交功能，包括查询、交易、智能合约操作等事务；
- c) 具备业务管理、服务集成、技术服务支持、治理和审计等功能；
- d) 具备事件管理、问题管理、安全管理、监控管理等功能。

6.1.3 服务接口层

服务接口层测试要求应包含但不限于：



- a) 具备账户信息查询、账本信息查询、事务操作处理、外部数据接入、接口服务能力管理、接口访问权限管理等接入管理功能；
- b) 具备节点服务器信息查询、节点服务启动关闭控制、节点服务配置、节点网络状态监控、节点授权管理等节点管理功能；
- c) 具备区块链系统链上内容发布与交互、对特定事务处理进行多签名权限控制设置、基于智能合约功能组件执行合约逻辑等账本应用功能。

6.1.4 核心功能层

核心功能层测试要求包含但不限于：

- a) 应具备多节点共识确认、独立节点的提交和记录信息有效性验证、共识机制容错、共识机制可扩展等共识机制功能；
- b) 应具备持久化存储账本记录、多节点拥有完整数据记录、自定义账本权限、节点数据一致性等账本记录功能；
- c) 应具备签名和验签等数字签名功能；
- d) 应具备统一账本记录、时序容错性、第三方时序服务等时序服务功能；
- e) 宜具备国际主流加密算法、国际主流商密算法、隐私保护算法、密钥管理等加密算法功能；
- f) 宜具备国际主流商密摘要算法、商密摘要算法、系统摘要算法验证等摘要算法功能；
- g) 宜具备智能合约形式化验证、合约虚拟机、系统外部数据和智能合约交互、智能合约防篡改、智能合约访问控制、智能合约升级和账本中写入合约等功能。

6.1.5 基础设施层

基础设施层测试要求应包含但不限于：

- a) 具备节点间安全通信、节点多播功能、节点动态管理等对等网络功能；
- b) 具备节点数据写入、查询及节点稳定存储等功能；
- c) 具备敏感数据安全存储功能；
- d) 具备数据防篡改、消息防篡改功能；
- e) 对于采取分库分表的数据存储方案，存储功能组件具备数据的分片及路由处理能力；
- f) 具备计算能力和环境支持，如容器技术、虚拟机技术、云计算技术等。

6.2 性能测试要求

6.2.1 通则

性能测试指标应包含时间特性、容量和资源利用性，表 1 按照 GB/T 29835.1—2013 结合区块链特性，规定了性能测试指标及其描述，具体测试项按附录 A 中表 A.2 执行。

表 1 性能测试指标及描述

序号	测试指标	测试指标描述
1	时间特性	响应时间：用户发起一个请求开始，服务器完成对该请求的处理并返回处理结果所经过的时间
		周转时间：执行一个事物所经过的时间，一个事物通常由多个操作步骤组成，周转时间是从第一个操作开始到最后一个操作完成所经过的时间
		吞吐率：单位时间内区块链系统处理完成的请求数量或任务数量

表 1 性能测试指标及描述（续）

序号	测试指标	测试指标描述
2	容量	最大并发用户数：区块链系统能够承受的同时使用区块链系统服务或资源的用户数的极限，超过该用户数，将导致区块链系统效率严重下滑，并可能导致崩溃、失效
		最大并发请求数：区块链系统能够承受的同时接收到的请求数极限，超过该请求数，将导致区块链系统效率严重下滑，并可能导致崩溃、失效
		事务吞吐容量：在一定时间单位内，区块链系统能够处理完成的最大事务量
		数据吞吐量：在一定时间单位内，区块链系统能够处理完成的最大数据量
		数据处理容量：对于指定的数据处理或数据存储功能，区块链系统能够处理的最大数据量
3	资源利用性	处理器平均占用率：区块链系统执行一组任务时，处理器所需时间与运行时间的平均比率
		内存平均占用率：区块链系统执行一组任务时，所需内存与可用内存的平均比率
		带宽占用率：区块链系统执行一组任务时，实际传输带宽与可用带宽的比率

6.2.2 测试要求

- 性能测试测试项应覆盖表 1 所规定的指标，测试要求包含但不限于：
- a) 时间效率，区块链系统执行某任务所需要的时间相关特性；
  - b) 处理效率，区块链系统在单位时间内处理的任务数量相关特性；
  - c) 用户容量，区块链系统能够承受的最大并发用户数量及最大并发请求数量；
  - d) 处理容量，区块链系统在给定时间内能够处理的任务量的极限；
  - e) 资源利用性，区块链系统现有资源利用情况的性能，包括 CPU、内存和带宽等；
  - f) 稳定性，区块链系统持续正常运行情况下处理事务的稳定性。

6.3 安全测试要求

6.3.1 网络安全等级保护测试

网络安全等级保护测试应按照 GB/T 22239—2019 的要求执行。

6.3.2 用户层

- 用户层安全测试内容应包含但不限于：
- a) 具备访问控制与授权机制，测试应用程序、网站、终端设备等不同登录方式，测试是否可建立不同的访问策略；
  - b) 具备私钥保护机制，测试私钥的生成、存储、使用、找回、销毁、更新等环节，对设计缺陷、私钥保存环境的恶意代码等进行测试；
  - c) 具备身份认证机制，测试管理成员的认证、授权、监控、审计等环节。

6.3.3 服务接口层

服务接口层安全测试要求包含但不限于：

- a) 应具备合理的加密算法和认证机制；
- b) 应具备隐私保护机制,宜采用同态加密、零知识证明等技术；
- c) 应具备存储和传输区块数据加密机制,宜采用国密算法；
- d) 应具备身份验证机制,宜采用数字证书和电子签名技术。

#### 6.3.4 核心功能层

核心功能层安全测试内容包含但不限于：

- a) 应具备高容错性的共识机制；
- b) 应具备抵御双花攻击、重放攻击、分叉攻击、贿赂攻击、算力攻击等攻击的能力；
- c) 宜具备两种(含两种)以上共识机制；
- d) 宜具备图灵完备、可验证和可审计的智能合约、外部查询和调用等操作；
- e) 智能合约应具备防止逻辑错误、函数错误、整数溢出、虚拟机和运行环境的漏洞等攻击的能力；
- f) 宜支持 SM2、SM3、SM4 等国密算法。

#### 6.3.5 基础设施层

基础设施层安全测试内容应包含但不限于：

- a) 具备 P2P 网络安全保障机制,防止 DDoS、女巫、日蚀等攻击；
- b) 具备硬件设备安全保障机制,防止 DNS 污染、路由广播、木马病毒等攻击。

#### 6.4 可靠性测试要求

可靠性测试内容应包含但不限于：



- a) 符合节点可靠性要求,包括新增节点基础事务完备性、账本信息一致性等,支持节点准入配置以及多节点共识完备；
- b) 符合事务执行可靠性要求,包括负载账户查询、负载区块查询、负载基础交易查询、负载基础交易等事务成功率及稳定性等；
- c) 符合加密技术可靠性要求,包括密钥管理方案、数据隐私保护、交易信息加密等；
- d) 符合智能合约可靠性要求,包括变更记录完备性、合约内容升级共识、外部数据交互、合约内容防篡改等要求；
- e) 符合区块链系统易恢复性要求,包括节点恢复能力、节点存储可恢复、区块链系统恢复后性能保障、恢复时间符合预置的要求等；
- f) 符合区块链系统容错性要求,包括共识可靠性、最大时失效和作恶节点容忍度。

### 7 测试程序

#### 7.1 概述

系统测试程序主要包含但不限于需求分析、策划设计、环境配置、测试执行、总结改进和测试管理,见图 2。



图 2 区块链系统测试流程

7.2 需求分析

需求分析阶段主要活动包含但不限于：

- a) 分析区块链系统测试的测试目的和必要性；
- b) 分析被测区块链系统相关技术文档，确定被测对象、测试类型和测试方法。

7.3 策划设计

策划设计阶段主要活动包含但不限于：

- a) 确定测试计划、测试方案、测试用例和测试说明；
- b) 规划测试时间及资金；
- c) 分析测试风险，制定风险应对方案；
- d) 分析测试环境要求；
- e) 调配测试环境资源，如硬件、软件、工具等；
- f) 建立测试环境，部署测试工具或软件；
- g) 组建测试团队，具体见表 2。

表 2 测试团队角色

工作角色	工作职责
测试负责人	管理监督测试项目，提供技术指导，获取测试资源，制定基线，技术协调，负责项目安全保密和质量管理
测试分析员	确定测试计划、测试内容、测试方法、测试数据生成方法、测试（软件、硬件）环境、测试工具，评价测试工作的有效性



表 2 测试团队角色（续）

工作角色	工作职责
测试设计员	设计测试用例,确定测试用例优先级,建立测试环境
测试开发工程师	编写测试辅助软件
测试员	执行测试,记录测试结果,编写测试报告
测试系统管理员	对测试环境和资产进行管理和维护
配置管理员	设置、管理和维护测试配置管理数据库。由系统开发方实施测试时,配置管理员应由本开发项目的管理员担任;由独立的测试组织实施测试时,宜配备测试活动的配置管理员
质量监督员	对测试过程、测试记录、判定结果进行监督,对仪器设备的运行过程进行监督,负责对测试过程中样品及资料的保密工作进行监督检查,对测试过程中实施全过程公正性及诚信度监督

7.4 测试执行

测试执行阶段主要活动包含但不限于:

- a) 根据测试计划、测试方案、测试用例和测试说明,在测试环境中执行测试用例;
- b) 人工或由测试环境自动判读测试结果;
- c) 根据期望测试结果和评估准则等,判定每个测试用例是否通过;
- d) 应准确记录测试结果;
- e) 当测试用例不通过时,宜根据不同的缺陷类型采取相应的措施;
- f) 若是测试工作缺陷(包含测试用例、测试数据、执行步骤、测试环境等),实施相应的变更;
- g) 若是系统缺陷,应在问题报告单中准确记录;
- h) 形成测试记录,至少包含但不限于测试用例标识、测试结果描述和发现的缺陷;
- i) 必要时,可开展回归测试。

7.5 总结改进

总结改进阶段主要活动包含但不限于:

- a) 分析总结测试报告及测试过程中发现的问题;
- b) 根据差异评价被测系统的设计和实现,制定系统改进建议;
- c) 改进优化被测系统。

7.6 测试管理

测试管理阶段主要活动包含但不限于:

- a) 实施过程管理,包含但不限于测试流程管理、测试人员管理、测试活动管理和测试资源管理;测试活动管理要求见 GB/T 8566—2022 中 6.1,测试资源管理要求参见 GB/T 8566—2022 中 6.2;
- b) 测试配置管理,由系统开发方组织实施的测试,宜将测试工作产品纳入项目配置管理;由测试组织实施的软件测试,宜建立配置管理库,将被测对象和测试工作产品纳入配置管理,配置管

理要求见 GB/T 20158—2006；

- c) 测试评审管理,主要包含但不限于:在测试执行前,对测试方案和测试用例等文档进行评审;在测试执行后,对测试结果和测试报告进行评审。

8 测试方法

8.1 功能测试

8.1.1 黑盒测试

区块链系统黑盒测试的方法包括但不限于:参照 GB/T 42752—2023 功能视图设计测试用例,采用黑盒测试技术,设计覆盖区块链系统功能实现的测试用例的方法,从功能实现的正确性、完整性、安全性等方面对区块链系统全部功能进行质量测试,并将功能性检测结果与该标准中的功能要求比较,评价该区块链系统功能是否符合该标准中的指标要求。

8.1.2 白盒测试

白盒测试方法包括但不限于:

- a) 优先选用自动化测试工具进行静态结构分析;
- b) 以静态分析的结果作为依据,用代码检查和动态测试的方式对静态分析结果进行进一步确认,提高测试效率及准确性;
- c) 使用多种覆盖率标准衡量代码的覆盖率。

8.2 性能测试

8.2.1 负载测试

负载测试方法包括但不限于:

- a) 对被测系统持续增加压力,直到性能指标超过预定指标或者某种资源使用已经达到饱和状态,找到系统的处理极限;
- b) 确定测试环境,需要考虑被测系统的业务压力量和典型场景,使得测试结果具有业务上的意义;
- c) 确定系统的性能容量,配合性能调优。

8.2.2 并发测试

通过模拟用户的并发访问,测试区块链系统能够产生的最大并发用户数。

8.3 安全测试

安全测试方法应包括但不限于:

- a) 使用安全扫描工具对系统进行扫描操作;
- b) 对难以实现自动化检测漏洞进行手工检测,分析或检查源程序的语法、结构、过程、接口等来检查程序的正确性;
- c) 利用模拟黑客攻击的方式,评估系统地域攻击的能力。

#### 8.4 可靠性测试

区块链可靠性测试应包括但不限于：

- a) 测试系统在负载状态下持续运行 12 h 的稳定性,记录过程中系统的运行状况；
- b) 使用系统不允许用户输入的异常值作为测试输入,测试系统的容错性；
- c) 在系统中植入故障,测试系统容错性和成熟性；
- d) 在一定负载下,长时间大容量运行某种业务,测试系统稳定性；
- e) 在一段时间内持续使用超过系统规格的负载进行测试,验证系统可靠性。





附 录 A  
(规范性)  
区块链系统功能测试和性能测试项列表

A.1 功能测试

表 A.1 规定了区块链系统功能测试项。

表 A.1 区块链系统功能测试项列表

序号	测试类别	测试项	测试子项
1	用户功能	用户界面	命令行交互功能
2			图形交互功能
3			应用程序接口交互功能
4		事务提交	事务提交功能
5	业务功能	区块链服务选择	区块链服务选择功能
6		区块链服务订购	区块链服务订购功能
7		使用区块链账务	使用区块链账务功能
8		财务管理	区块链财务管理功能
9	管理功能	成员管理	身份管理
10			权限管理
11			数据保密
12			可审计功能
13		监控管理	故障监测
14			网络运行状态监控
15		事件管理	预定义事件功能
16			自定义事件功能
17		问题管理	网络问题跟踪及报告
18		安全管理	账号安全功能
19	接入管理	账户信息查询	账户体系相关的基本信息查询服务
20		账本信息查询	区块总高度查询服务
21			指定高度区块查询服务
22			区块标识查询服务
23			事务查询服务
24		事务操作处理	特定事务操作请求提交功能
25		接口服务能力管理	接口调用频度管理功能
26			接口查询缓存管理功能
27		接口访问权限管理	较低等级权限接口访问
28			较高等级权限接口访问

表 A.1 区块链系统功能测试项列表（续）

序号	测试类别	测试项	测试子项
29	节点管理	节点服务器信息查询	节点状态信息查询
30		节点服务启动关闭控制	节点启动功能
31			节点服务启动功能
32			节点服务关闭功能
33			节点关闭功能
34		节点服务配置	节点参与共识算法配置
35	节点网络状态监控		节点连接数量配置
36			节点对外提供接入服务配置
37		节点网络状态监控	节点连通状况监控服务
38			节点连接数量监控服务
39			节点带宽监控服务
40		节点授权管理	准入配置
41			准出配置
42			被测试节点事务处理
43			被测试节点以外节点的事务记录
44			账本允许查询授权配置
45			账本禁止查询配置
46	账本应用	链上内容发行和交换	链上内容发布功能
47			链上内容增加功能
48			链上内容撤销功能
49			链上内容分配功能
50			链上内容交换功能
51		共识前的逻辑验证和共识后的结果验算	共识前特定标识资产的逻辑验证
52			共识前资产数额逻辑验证
53			共识后的结果验算
54		可对特定事务处理进行多签名权限控制设置	可对多签名权限控制设置
55			可对特定事务处理进行多签名
56			可对多签名事务处理进行验证
57		执行合约逻辑	可基于智能合约功能组件执行合约逻辑
58	共识机制	多节点共识确认	支持多个节点参与共识和确认
59		独立节点的提交信息有效性验证	正确事务逻辑验证
60			错误事务逻辑验证
61		独立节点记录信息需通过共识	防止独立节点未经共识进行信息记录或修改
62		共识机制容错性	物理故障导致的非恶意错误容错性

表 A.1 区块链系统功能测试项列表（续）

序号	测试类别	测试项	测试子项
63	账本记录	持久化存储账本记录	支持持久化存储账本记录
64		多节点拥有完整的数据记录	支持多节点拥有完整的区块记录
65			支持多节点拥有完整的数据记录
66		自定义账本权限	支持向获得授权者提供真实的数据记录
67		各节点数据一致性	确保有相同账本记录的各节点数据一致性
68	密码服务	支持国际主流加密算法和商密	查询文档验证支持国际主流加密算法和商密算法
69		具备明确的密钥管理方案管理用户数据和私钥	持有正确密钥的访问者能解密和访问数据
70			持有错误密钥访问者不能解密和访问数据
71		具备抵御破解的能力	用如零知识证明、环签名、同态加密等隐私保护算法
72	摘要	支持国际主流商密摘要算法	查询文档并对比区块链系统与第三方的摘要算法
73		摘要算法应具备抵御破解的能力	区块链系统的摘要算法应用于微小差异的结果
74	数字签名	支持国际主流商密数字签名算法	查询文档验证支持国际主流商密数字签名算法
75		数字签名和验签	对区块链上数据进行签名
76			对区块链上已签名数据进行验签
77	时序服务	统一账本记录	支持统一账本记录时序
78		时序容错性	具备时序容错性
79		第三方时序服务	必要时,支持集成可信第三方时序服务
80	智能合约	开发运行环境	提供编程语言支持
81			提供配套的集成开发环境
82		合约内容静态和动态检查	支持合约内容静态和动态检查
83		支持运行载体	提供运行载体支持,如虚拟机等
84		外部数据源和智能合约交互	智能合约与外部数据源交互的影响范围应仅限于智能合约范围内
85		合约防篡改	防止对合约内容进行篡改
86		多方共识下的合约升级	支持多方共识下的合约内容升级
87		账本中写入合约内容	支持向账本中写入合约内容
88	对等网络	节点之间的高效安全通信	能够进行点对点之间的通信
89			点对点之间的通信接口
90			能够进行点对点之间的安全通信
91		点对点通信多播能力	能够提供点对点通信基础的多播能力
92		动态增删节点	支持对节点的动态添加的识别
93			支持对节点的动态减少的识别

表 A.1 区块链系统功能测试项列表（续）

序号	测试类别	测试项	测试子项
94	储存	节点数据写入正确性	对等网络能够被每个节点部署并使用
95			对等网络能够被每个节点查询
96		节点高效稳定存储	能够提供高效稳定的数据服务
97			能够提供安全的数据服务
98	计算	区块链节点运行环境监控	对区块链系统提供运行环境支持
99		区块链节点计算能力	对等网络中,计算能力能够满足每个节点要求

A.2 性能测试

表 A.2 规定了区块链系统性能测试项。

表 A.2 区块链系统功能测试项列表

序号	测试项	测试子项
1	时间效率测试	交易转账事务请求时间效率
2		历史信息查询事务时间效率
3		区块信息查询事务时间效率
4		账户信息查询事务时间效率
5	处理效率	交易转账事务请求处理效率
6		历史信息查询事务处理效率
7		区块信息查询事务处理效率
8		账户信息查询事务处理效率
9	用户容量	交易转账事务请求用户容量
10		历史信息查询事务用户容量
11		区块信息查询事务用户容量
12		账户信息查询事务用户容量
13	处理容量	交易转账事务请求处理容量
14		历史信息查询事务处理容量
15		区块信息查询事务处理容量
16		账户信息查询事务处理容量
17	资源利用性	交易转账资源利用性
18		历史信息查询资源利用性
19		区块信息查询资源利用性
20		账户信息查询资源利用性
21	稳定性	稳定性

参 考 文 献

[1] GB/T 5271.18—2008 信息技术 词汇 第 18 部分:分布式数据处理

[2] GB/T 8566—2022 系统与软件工程 软件生存周期过程

[3] GB/T 20158—2006 信息技术 软件生存周期过程 配置管理

[4] GB/T 32399—2015 信息技术 云计算 参考架构

[5] GB/T 35273—2020 信息安全技术 个人信息安全规范

[6] GB/T 42752—2023 区块链和分布式记账技术 参考架构

[7] GB/T 43572—2023 区块链和分布式记账技术 术语

[8] ISO/IEC/IEEE 29119-1:2022 Software and systems engineering—Software testing—  
Part 1: General concepts

---