ICS 35.240
CCS L70

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息技术 区块链和分布式记账技术 系统测试要求

Information Technology—Blockchain and distributed ledger technology—System testing requirements

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

发布

国家市场监督管理总局
国家标准化管理委员会

目　次

前　言

本标准按照GB/T 1.1-2020给出的规则起草。

本标准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）提出并归口。

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这些专利的责任。

本标准负责起草单位：中国电子技术标准化研究院、厦门安妮股份有限公司、京东数字科技控股股份 有限公司、中国平安保险（集团）股份有限公司、杭州趣链科技有限公司、浙江大学、北京中电普华 信息技术有限公司、易见供应链管理股份有限公司、智度科技股份有限公司。

本标准主要起草人：李鸣、王晨辉、郝汉、蔡亮、张栋、冯承勇、陶祥忍、靳涵、 陈晓丰、赵伟、颜爱军、张春光、王思宁、刘天成、李努锲、王鹏飞。

区块链和分布式记账技术 系统测试要求

1 范围

本文件规定了区块链系统的测试原则，规定了功能测试、性能测试、安全测试、可靠性测试、合规性测试的要求。

本文件适用于：

a) 为区块链系统建设方提供参考依据；

b) 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指导；

c) 为区块链系统使用方开展系统选型和验收提供依据；

d) 为行业主管部门的管理监管提供技术支撑。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文 件。凡是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 20158-2006 信息技术 软件生存周期过程配置管理

GB/T 25069-2022 信息安全技术 术语

GB/T 32399-2015 信息技术 云计算 参考架构

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 35273-2017 信息安全技术个人信息安全规范

GB/T XXXXXXXXXX 区块链和分布式记账技术 参考架构

ISO 22739:2020 Blockchain and distributed ledger technologies-Vocabulary

3 术语和定义

GB/T25069-2010、GB/T5271.18-2008、GB/T32399-2015、GB/T11457-2006、T/CESA 6001-2016、ISO/IEC/IEEE 29119-1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。

[GB/T 5271.18-2008，定义 2.18.04.05]

3.2

加密 encipherment / encryption

对数据进行密码变换以产生密文的过程。

[GB/T 25069-2022，定义 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。

[GB/T 32399-2015，定义 3.2.1]

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。

[GB/T 25069-2022，定义3.576]

3.5

摘要算法 digest algorithm

摘要函数 digest function

Hash 函数 hash function

通常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上。

[ISO 22739:2020，定义 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。

[GB/T 11457-2006，定义 2.669]

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。

[GB/T 11457-2006，定义 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。

[ISO/IEC/IEEE 29119-1，定义 4.28]

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。

[GB/T 11457-2006，定义 2.1334]

3.11

合规性 compliance

符合当地的法律、规则和准则。

4 缩略语

下列缩略语适用于本文件。

AML：反洗钱（Anti-Money Laundering）

ATA：反避税（Anti-Tax Avoidance）

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

DNS：域名系统（Domain Name Server）

KYC：了解你的客户（Know Your Customer）

P2P：点对点（Peer to Peer）

SLA：服务等级协议（Service Level Agreement）

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）

TPS：每秒处理事务数（Transaction per Second）

5 测试原则

在区块链系统测试过程中，应遵循下列原则：

a) 客观性原则：确切了解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，不应利用这些信息进行任何非授权的活动，测试报告不应扩散给未经授权的第三方；

c) 规范性原则：测试应以标准为依据，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。

6 测试体系

区块链系统测试体系包含功能测试、性能测试、安全测试、可靠性测试，以及合规性测试，见图1。区块链系统测试程序见附录A，区块链系统测试方法见附录B。

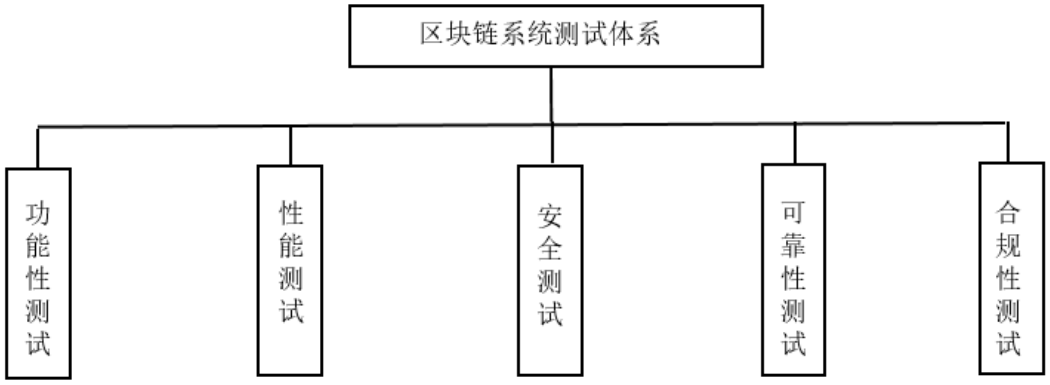

图1 区块链系统测试体系

7　功能性试

7.1　通则

功能测试应覆盖区块链系统功能架构中的基础层、核心层、服务层、用户层，图2规定了每层对应的具体功能测试类。功能测试相关测试项详应符合附录C的规定。

图2　区块链系统功能架构

7.2.2　测试内容

7.2.2.1　用户层（达闼机器人-谢老师）

用户层测试内容包含但不限于：

a) 应以送测产品的用户功能列表为准，可支持区块链系统的命令行交互、图形交互、应用接口交互、等用户功能；
b) 宜以送测产品的业务功能列表为准，支持系统的区块链服务选择、服务订购、账务、财务管理等业务功能；
c) 应支持系统成员管理、监控管理、事件管理、问题管理、安全管理等管理功能。

7.2.2.2　服务层（天河国云-杨征）

服务层测试内容包含但不限于：

a) 应支持账户信息查询、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) 应支持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) 宜支持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。

7.2.2.3 核心层（蚂蚁-昌文婷）

核心层测试内容包含但不限于：
a) 应支持区块链系统多节点共识确认、独立节点的提交和记录信息有效性验证、共识机制容错、共识机制可拓展等共识机制功能；
b) 应支持区块链系统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) 应支持区块链系统签名和验签等数字签名功能；
d) 应支持统一账本记录、时序容错性、第三方时序服务等时序服务功能；
e) 宜支持国际主流加密算法、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) 宜支持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) 宜支持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、智能合约业务隔离、智能合约升级和账本中写入合约等功能。

7.2.2.4 基础层（零数科技）

基础层测试内容包含但不限于：
a) 应支持区块链系统节点间安全通信、节点多播功能、节点动态管理等对等网络功能；
b) 应支持区块链系统节点数据写入、查询及节点稳定存储等功能；
c) 应支持区块链系统敏感数据安全存储功能；
d) 应支持区块链系统数据防篡改、消息防篡改功能；
e) 对于采取分库分表的数据存储方案，存储功能组件还应包括数据的分片及路由处理能力；
f) 应具备一定的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；
g) 应支持区块链系统节点运行环境监测和节点计算能力监测等功能。

8 性能测试

8.1 通则

性能测试指标应包含时间特性、资源利用性和容量，表1规定了性能测试指标及其描述。性能测试相关测试项应符合附录C.2的规定。

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	平均响应时间：执行一个请求，记录从提交请求开始到完成该请求处理并返回处理结果所需的平均时间
		平均吞吐量：区块链系统单位时间内处理的平均事务数量
2	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
3	容量	事务处理容量：在要求的负载下，单位时间内处理完成最大事务的数量 **注：**本文件中事务通常指交易或者查询操作

8.2 测试内容

性能测试测试项应覆盖表1所规定的指标，测试内容应包含但不限于：

a) 账户单次转账性能和不同负载状态下的账户转账性能；
b) 智能合约单次转账性能和不同负载状态下的智能合约转账性能；
c) 随机调用智能合约的单次转账性能和在不同负载下的智能合约转账性能；
d) 单次交易查验性能和不同负载状态下的交易查验性能；
e) 单次区块查验性能和不同负载状态下的区块查验性能；
f) 单次账户查验性能和系统不同负载转状态下的账户查验性能；
g) 系统在负载状态下处理混合事务的性能；

9 安全测试

9.1 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。

9.2 区块链安全测试

9.2.1 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，针对应用程序、网站、终端设备等不同登录方式建立不同的访问策略；
b) 具备私钥保护机制，规范管理私钥的生成、存储、使用、找回、销毁、更新等环节，同时重点关注设计缺陷、私钥保存环境的恶意代码等，避免上述环节中存在设计缺陷、恶意代码等问题；
c) 具备身份认证机制，规范管理成员的认证、授权、监控、审计等环节。

9.2.2 服务层

服务层安全测试内容应包含但不限于：

a) 具备合理的加密算法和认证机制保证各节点访问安全；
b) 具备隐私保护机制保护事务数据的隐私，宜采用同态加密、零知识证明等技术；
c) 支持对存储和传输的区块数据进行加密，宜采用国密算法；
d) 具备身份验证机制，宜采用数字证书和电子签名技术。

9.2.3 核心层

核心层安全测试内容包含但不限于：

a) 应支持具备容错能力的共识机制；
b) 应能防止双花攻击、重放攻击、分叉攻击、贿赂攻击、算力攻击等攻击；

c) 宜支持多种共识机制的切换；
d) 宜具备图灵完备、可验证和可审计的智能合约，支持外部查询和调用等操作，
e) 智能合约应能防止逻辑错误、函数错误、整数溢出、虚拟机和运行环境的漏洞等攻击；
f) 宜支持 SM2、SM3、SM4 等国密算法。

9.2.4 基础层

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

10 可靠性测试

可靠性测试内容包含但不限于：
a) 应满足节点可靠性要求，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) 应满足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) 应满足加密技术可靠性要求,包括秘钥管理方案、数据隐私保护、交易信息加密等；
d) 应满足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) 应满足系统易恢复性要求，包括节点恢复能力、节点存储可恢复、系统恢复后性能保障、恢复时间符合预置的要求等；
f) 应满足系统容错性要求，包括共识可靠性、最大时失效和作恶节点容忍度、多节点投票回滚功能等。

11 合规性测试

11.1 组织和人员

组织和人员合规性测试内容包含但不限于：
a) 组织的信息披露应真实、可靠、完整、及时；
b) 组织的信息披露应包括资质证明、财务和资产数据、经营业绩、信用记录等；
c) 组织应满足主体监管要求，记录平台的各参与方信息，以备查证；
d) 组织应建立知识产权和专利保护机制，保护区块链系统相关知识产权和专利；
e) 组织宜获得权威第三方的认证和认可资质；
f) 区块链相关人员应具备区块链相关知识和技能；
g) 区块链相关人员宜参加第三方的培训或认证，并获得资质和证书。

11.2 技术和平台

技术和平台测试内容包含但不限于：
a) 当采用开源框架时，应满足所采用区块链系统开源框架的开源协议要求；
b) 应具备完善的身份认证机制，宜采用前台自愿，后台实名注册的原则；
c) 应建立密码体系，能够按照不同业务需求和当地法规要求采用合规的密码标准，宜支持不同密码算法的灵活切换；

d) 应建立身份认证 KYC 机制，为合规监管提供技术支撑；
e) 应明确数据归属权和隐私保护机制，保障数据在共享、流动和交换过程中相关主体的权益；
f) 应建立隐私保护机制，防止未授权的数据跨境流动。

11.3 服务和运营

服务和运营测试内容包含但不限于：
a) 应建立区块链系统服务质量保障机制，满足服务水平协议 SLA；
b) 应满足区块链系统相关备案要求，获得备案资质；
c) 宜获得权威第三方的测试和认证；
d) 数字资产发行及运营服务方应主动向相关监管机构报备，并主动加入相应的监管体系。

附录 A
（资料性附录）
区块链系统测试程序

A.1 概述

区块链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A.1。

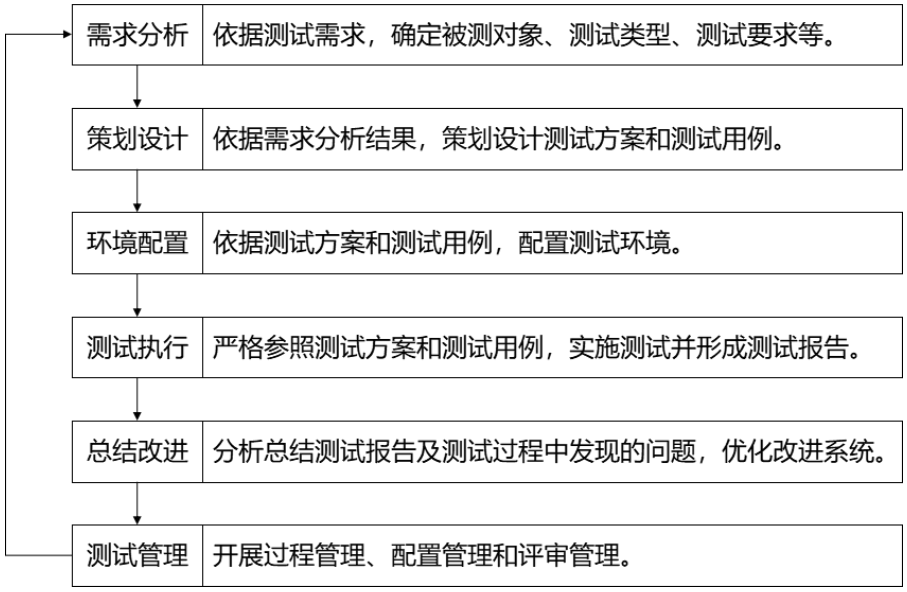

图 A.1 区块链系统测试流程

A.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) 分析被测系统相关技术文档，确定被测对象、测试类型和测试方法。

A.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，具体如表 B.1。

表 A.1 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

工作角色	工作职责
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
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。由区块链系统开发方实施测试时，配置管理员应由本开发项目的配置管理员担任；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。

A.5 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。

A.6 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) 改进优化被测区块链系统。

A.7 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。测试活动管理要求参见 GB/T 8566-2007 中 7.1，测试资源管理要求参见 GB/T 8566-2007 中 7.5；
b) 测试配置管理，由区块链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；由对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，配置管理要求参见 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。

附录 B
（资料性附录）
区块链系统测试方法

B.1 功能测试

B.1.1 黑盒测试

区块链系统黑盒测试的方法包括但不限于：按照T/CESA 6001-2016 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，从功能实现的功能正确性、功能实现的完整性、安全性等方面对区块链系统全部功能性进行质量测试，并将功能性检测结果与标准中的功能要求比较，评价该区块链系统功能是否符合标准中的指标要求。

B.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来进行静态结构分析；
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。

B.2 性能测试

B.2.1 负载测试

负载测试方法包括但不限于：

a) 在被测系统上不断增加压力，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，为系统调优提供数据。
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。

B.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数。

B.2.3 稳定性测试

稳定性测试方法包括但不限于：

a) 记录系统在负载状态下持续一段时间的稳定性，一般进行 3*24 小时；
b) 测试过程中需要关注系统的运行状况。

B.3 安全测试

安全测试方法包括但不限于：

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以下手工检测，如通过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，来评估计算机网络系统安全性能的方法。

B.4 可靠性测试

区块链可靠性测试应包括但不限于：
a) 使用系统不允许用户输入异常值作为测试输入测试系统的容错性；
b) 在系统中植入故障，测试系统容错性和成熟性；
c) 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；
d) 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。

B.5 合规性测试

合规性测试方法宜包括：
a) 收集和分类区块链相关法律、法规、标准和规范，建立合规知识库；
b) 梳理知识库库文件的控制点，建立合规控制矩阵；
c) 根据控制点建立评价指标体系和控制方法；
d) 采用访谈、调查、检查、观察、自动化工具等方法开展合规性测试。

附录 C
（规范性附录）
区块链系统功能测试和性能测试项列表

C.1 功能测试

表C.1规定了区块链系统功能测试项。

表 C.1 区块链系统功能测试项列表

序号	测试类	测试项	测试子项	类型
1	用户功能	用户界面	命令行交互功能	必选
2			图形交互功能	可选
3			应用程序接口交互功能	可选
4		事务提交	事务提交功能	必选
5	业务功能	区块链服务选择	区块链服务选择功能	可选
6		区块链服务订购	区块链服务订购功能	可选
7		使用区块链账务	使用区块链账务功能	可选
8		财务管理	区块链财务管理功能	可选
9	管理功能	成员管理	身份管理	必选
10			权限管理	必选
11			数据保密	必选
12			可审计功能	可选
13		监控管理	故障监测	必选
14			网络运行状态监控	可选
15		事件管理	预定义事件功能	必选
16			自定义事件功能	可选
17		问题管理	网络问题跟踪及报告	必选
18		安全管理	账号安全功能	必选

序号	测试类	测试项	测试子项	类型
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	必选
20		账本信息查询	区块总高度查询服务	必选
21			指定高度区块查询服务	必选
22			区块标识查询服务	必选
23			事务查询服务	必选
24		事务操作处理	特定事务操作请求提交功能	必选
25		接口服务能力管理	接口调用频度管理功能	可选
26			接口查询缓存理功能	可选
27		接口访问权限管理	较低等级权限接口访问	可选
28			较高等级权限接口访问	可选
29	节点管理	节点服务器信息查询	节点状态信息查询	必选
30		节点服务启动关闭控制	节点启动功能	必选
31			节点服务启动功能	必选
32			节点服务关闭功能	必选
33			节点关闭功能	必选
34		节点服务配置	节点参与共识算法配置	必选
35			节点连接数量配置	可选
36			节点对外提供接入服务配置	可选
37		节点网络状态监控	节点连通状况监控服务	必选
38			节点连接数量监控服务	必选

序号	测试类	测试项	测试子项	类型
39			节点带宽监控服务	必选
40		节点授权管理	准入配置	必选
41			准出配置	必选
42			被测试节点事务处理	必选
43			被测试节点以外节点的事务记录	必选
44			账本允许查询授权配置	可选
45			账本禁止查询配置	可选
46	账本应用	链上内容发行和交换	链上内容发布功能	必选
47			链上内容增加功能	必选
48			链上内容撤销功能	可选
49			链上内容分配功能	必选
50			链上内容交换功能	必选
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	必选
52			共识前资产数额逻辑验证	必选
53			共识后的结果验算	必选
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	可选
55			可对特定事务处理进行多签名	可选
56			可对多签名事务处理进行验证	可选

序号	测试类	测试项	测试子项	类型
57		执行合约逻辑	可基于智能合约功能组件执行合约逻辑	可选
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	必选
59		独立节点的提交信息有效性验证	正确事务逻辑验证	必选
60			错误事务逻辑验证	必选
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	必选
62		共识机制容错性	物理故障导致的非恶意错误容错性	必选
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	必选
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	必选
65			支持多节点拥有完整的数据记录	必选
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	必选
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	必选
68	加密	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	可选
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	必选
70			持有错误密钥访问者不能解密和访问数据	必选

序号	测试类	测试项	测试子项	类型
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	可选
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	可选
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	可选
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	可选
75		数字签名和验签	对区块链上数据进行签名	可选
76			对区块链上已签名数据进行验签	可选
77	时序服务	统一账本记录	支持统一账本记录时序	必选
78		时序容错性	具备时序容错性	必选
79		第三方时序服务	必要时，支持集成可信第三方时序服务	可选
80	智能合约	开发运行环境	提供编程语言支持	可选
81			提供配套的集成开发环境	可选
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	可选
83		支持运行载体	提供运行载体支持，如虚拟机等	可选
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	可选
85		合约防篡改	防止对合约内容进行篡改	可选

序号	测试类	测试项	测试子项	类型
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	可选
87		账本中写入合约内容	支持向账本中写入合约内容	可选
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	必选
89			点对点之间的通信接口	必选
90			能够进行点对点之间的安全通信	必选
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	必选
92		动态增删节点	支持对节点的动态添加的识别	必选
93			支持对节点的动态减少的识别	必选
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	必选
95			对等网络能够被每个节点查询	必选
96		节点高效稳定存储	能够提供高效稳定的数据服务	必选
97			能够提供安全的数据服务	可选
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	必选
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	必选

C.2 性能测试

表C.2规定了区块链系统性能测试项。

表 C.2 区块链系统功能测试项列表

序号	测试项	测试子项	类型
1	基本账户转账性能测试	基本账户单次转账测试	必选
2		基本账户单次转账负载测试	
3	智能合约 转账性能测试	智能合约单次转账测试	必选
4		智能合约单次转账负载测试	
5	随机合约调用 性能测试	随机合约单次转账测试	必选
6		随机合约单次转账负载测试	必选
7	交易查验	单次账户查验测试	必选
8		单次账户查验负载测试	
9	区块查验	单次区块查验测试	必选
10		单次区块查验负载测试	
11	账户查验	单次账户查验测试	必选
12		单次账户查验负载测试	
13	混合负载测试	混合交易负载测试	必选
14		混合查询负载测试	
15		混合事务负载测试	
16	稳定性测试	稳定性测试	必选

参 考 文 献

[1] GB/T 9386-2008 计算机软件测试文件编制规范
[2] GB/T 11457-2006 信息技术 软件工程术语
[3] GB/T 34960.1-2017 信息技术服务 治理 第1部分：通用要求
[4] GB/T 34960.3-2017 信息技术服务 治理 第3部分：绩效评价
[5] GB/T 34960.4-2017 信息技术服务 治理 第4部分：审计导则
[6] GB/T 37961-2019 信息技术服务 服务基本要求
[7] GB/T 37696-2019 信息技术服务 从业人员能力评价要求
[8] 《企业每部控制基本规范》 中国人民共和国财政部[财会[2008]7号]2008年5月22日
[9] 《商业银行信息科技风险管理指引》 国务院国有资产监督管理委员会[国资发改革[2009]19号]2009 年 6 月 1 日
[10] GB/T 25069-2010 信息安全技术 术语
[11] GB/T 5271.1-2000 信息技术 词汇
[12] GB/T 11457-2006 信息技术 软件工程术语