

ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

团 体 标 准

T/GDAQIXXXXX—XXXX

基于区块链应用程序的通用测试标准

点击此处添加标准英文译名

点击此处添加与国际标准一致性程度的标识

文稿版次选择

—XX—XX 发布

XXXX—XX—XX 实施

广东省质量检验协会 发布

目 次

前 言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 系统边界 2

5 质量模型 2

6 测试要求 3

7 测试过程 17

附录 A（资料性附录） 缺陷严重级别说明表 19

附录 B（资料性附录） 测试结果判定表 21

前 言

本标准根据GB/T 1.1—2020给出的规则起草。

本标准由XXXX提出。

本标准由广东省质量检验协会归口。

本标准起草单位：

本标准主要起草人：

基于区块链应用软件的通用测试标准

1 范围

本标准规定了基于区块链应用软件的术语和定义、质量模型、测试要求以及测试过程等。
本标准适用于基于区块链应用软件的通用测试方法。

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，仅所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 25000.10-2016系统与软件工程系统与软件质量要求和评价（SQuaRE）第10部分：系统与软件质量模型

GB / T 25000.51-2016系统与软件工程系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

T/CESA 6001-2016 区块链参考架构

3 术语和定义

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。

3.2

区块链平台blockchain platform

实现区块链的信息化平台。

3.3

区块头block header

区块头包含当前区块的属性信息和前一个区块顺序固定信息。属性信息包括当前区块的时间戳、区块序号等。前一个区块顺序固定信息，一般是用能唯一标识前一个区块特征的hash值代表。

3.4

共识节点consensusnode

负责账本数据一致性的节点。

3.5

共识协议consensus protocol

分布式账本系统中各节点间为达成一致采用的计算方法。

3.6

智能合约Smart contract

以数字形式定义的能够自动执行条款的合约。

注：在区块链技术领域，智能合约是指基于预订事件触发、不可篡改、自动执行的计算机程序。

3.7

加密encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

3.8

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。

4 系统边界

区块链平台是实现区块链的信息化平台，其主要提供共识服务、链式数据结构（分布式账本）、身份管理、权限控制、加密服务、智能合约服务等功能支持，以及API以及扩展能力等。区块链应用软件系统是基于业务需求在区块链平台上开发的应用软件系统，通过区块链平台提供的接口服务与区块链平台进行集成，并在业务应用与区块链平台账本间实现数据的交互，以达成具体的业务应用目标。区块链技术在金融服务、供应链管理、文化娱乐、智能制造、社会公益和教育就业等有广泛的应用。

区块链应用软件系统架构大致分为4层：用户层、服务层、核心层、基础层。

- a) 用户层包括用户功能、业务功能和管理功能；
- b) 服务层包括接入管理、节点管理和账本应用功能；
- c) 核心层则包括共识机制、账本技术、加密、数字签名、摘要、时序服务以及智能合约功能；
- d) 基础层包括对等网络、存储服务以及计算功能。

具体如图1所示：

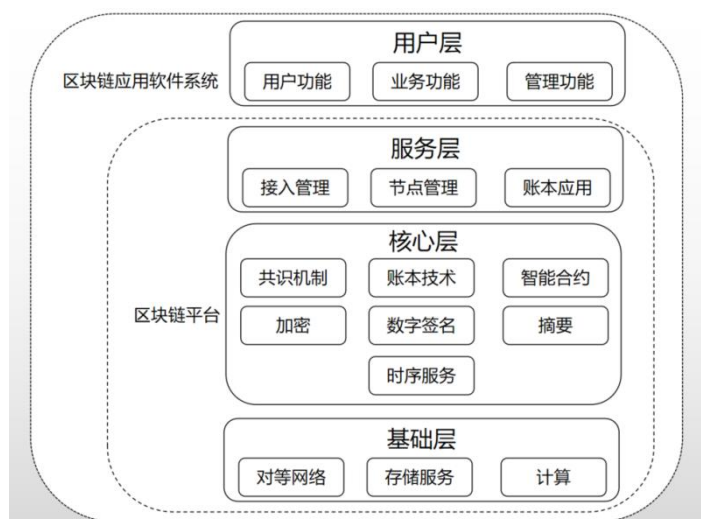


图1 区块链应用软件系统架构图

5 质量模型

本标准参考软件GB/T 25000.10-2016中的质量模型，分别从功能性、性能效率、兼容性、易用性、可靠性、信息安全性、维护性和可移植性八个方面阐述区块链应用软件系统测试要求。其中区块链应用软件系统质量模型如下图2所示。

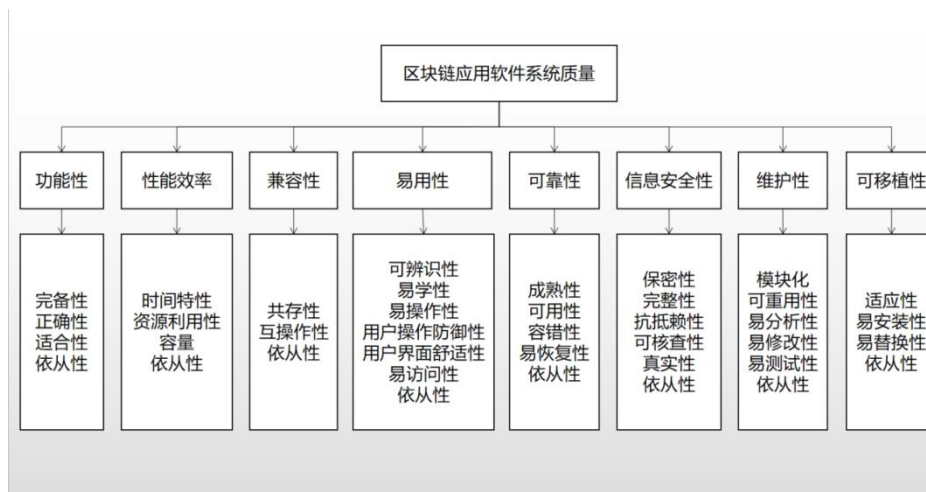


图2 区块链应用软件系统质量模型

6 测试要求

6.1 功能性

区块链应用软件基本功能测试可参见GB/T 25000.51-2016 系统与软件工程系统与软件质量要求和评价(SQuaRE)第51部分：就绪可用软件产品(RUSP)的质量要求和测试细则中相关要求并根据应用软件系统的实际功能进行测试，同时其功能测试还需包括如下内容：

- a) 共识机制
- b) 智能合约
- c) 节点间通信
- d) 账本技术
- e) 成员管理
- f) 状态管理
- g) 接口管理

6.1.1 共识机制

共识机制是区块链网络中各节点对在区块链应用软件系统中进行事务或状态的验证、记录、修改等行为达成一致确认的方法。不同区块链应用软件系统，会根据自身的业务需求而选择不同的共识算法来实现共识机制，因此，共识机制的功能测试点主要包括如下：

- a) 区块链应用软件系统如果支持多种共识算法，则需测试：
 - 1) 相关文档是否说明共识算法切换方式以及条件；
 - 2) 切换共识机制后，全网是否能达到共识且系统正常运行。
- b) 区块链应用软件系统的任意节点发起交易更新账本后，每个节点的交易状态写操作结果是否一致，每个节点的最终状态是否一致；
- c) 区块链应用软件系统的任意节点出现异常情况（如节点断电、重启、网络波动等）下，每个节点恢复后，其节点数据能否正常恢复，交易的状态是否一致，能否参与共识流程；

- d) 同样的交易在相同/不同节点多次运行，每个节点的交易执行结果是否唯一且一致；
- e) 任意节点发起交易，网络上各个节点均可终止交易；
- f) 区块链应用软件系统共识算法如果限制节点数量，则需测试：
 - 1) 相关文档是否声明共识算法最少参与的节点数量，且在最少节点数量上能否达成共识，系统正常运行；
 - 2) 相关文档是否声明共识算法最多支持的节点数量，且在最多节点数量上能否达成共识，系统正常运行。
- g) 区块链应用软件系统共识机制的容错阈值测试包括如下：
 - 1) 相关文档是否声明共识机制的容错阈值，即可接受的故障或恶意共识节点的比例；
 - 2) 当故障/恶意节点数<阈值时，是否可达成共识；
 - 3) 当故障/恶意节点数>阈值时，是否不可达成共识。

6.1.2 智能合约

智能合约是一种以数字形式定义的承诺，不同区块链应用软件系统，会根据自身的业务需求而有选择性地提供智能合约功能，其功能测试点主要包含如下：

- a) 正确调用智能合约，是否能调用成功且获得正确结果；
- b) 错误调用智能合约，是否调用失败并给出对应提示信息；
- c) 在不同节点上调用执行智能合约，结果是否一致；
- d) 多个节点同时调用执行智能合约，结果是否一致；
- e) 区块链应用软件系统调用智能合约执行异常操作能否正常撤回；
- f) 区块链应用软件系统升级后，能否正确运行智能合约；
- g) 区块链应用软件系统如果支持多种智能合约，则需要测试：
 - 1) 相关文档是否说明不同智能合约执行环境的隔离方法；
 - 2) 不同智能合约的业务数据：
 - 存储是否隔离，且未经授权不可访问；
 - 运行是否隔离，传输互不干扰。
- h) 在部署和调用执行智能合约时，是否建立严格有效的授权控制机制，即成员是否只能在授权范围内部署、调用、执行智能合约。
- i) 生命周期管理
 - 1) 区块链应用软件系统是否提供智能合约全生命周期管理，包括部署、运行、升级、冻结、解冻以及废止等一系列功能管理；
 - 2) 授权用户是否只能在授权节点部署智能合约；
 - 3) 未授权用户或未授权节点是否不可部署智能合约；
 - 4) 不同节点部署的智能合约是否一致且标识唯一；
 - 5) 智能合约升级/重新部署后，原智能合约的数据是否能正确迁移至新智能合约；
 - 6) 智能合约冻结后，是否不可提供服务；
 - 7) 智能合约冻结后是否可解冻，解冻后是否可重新提供服务；
 - 8) 智能合约废止后，是否不可提供服务；
 - 9) 交易信息是否包含智能合约版本信息；

6.1.3 节点间通信

区块链节点通常包括共识节点和接入节点。其中共识节点参与共识过程，生成区块；接入节点用于外部应用系统同步账本信息和提交事务处理。并由对等网络协议组织各个网络中的节点，节点间通过点对点通信协议完成信息交换。节点的功能测试点主要包括如下内容：

- a) 是否可动态配置节点通信的组网方式；
- b) 任意节点发生故障，是否不影响其他节点间通信；
- c) 节点是否有心跳机制：通过心跳机制维护节点状态，定时广播，确保状态同步和账本的一致性；
- d) 节点是否有异常恢复方案，如节点状态检查、定时广播、区块状态同步、异常连接自动断开，自动重连等，确保节点异常恢复后能迅速与其他节点建立连接进行通信；
- e) 消息转发的接收节点是否可配置，配置为接收节点后，该节点能否收发消息；
- f) 网络消息标识是否唯一；
- g) 同一消息在转发前后是否一致；
- h) 消息转发范围，则需测试：
 - 1) 相关文档是否明确定义消息转发范围；
 - 2) 在范围内，是否可接收到转发消息；
 - 3) 在范围外，是否无法接收到转发消息。
- i) 接受节点异常情况（断电、重启、网络波动等）恢复后，能否恢复转发消息功能；
- j) 节点加入
 - 1) 新节点是否可动态加入网络，且不影响系统通信；
 - 2) 新节点是否通过共识（共识或记账节点多方审核）后才可加入网络；
 - 3) 新节点的加密算法是否与加入的网络中的加密算法保持一致才可加入网络；
- k) 节点退出
 - 1) 不同类型/数量的节点是否可动态退出网络，且不影响系统通信；
 - 2) 节点退出后重新加入网络，是否通过共识（共识或记账节点多方审核），才可加入网络；
 - 3) 节点退出重新加入网络后，节点能否正常运行；与其他节点恢复通信后，节点账本数据是否与其他节点保持一致，且最终状态也保持一致。

6.1.4 账本技术

账本技术是指区块链中分布式数据的存储机制，通过不同节点对账本的共同记录与维护，形成区块链系统中数据的公共管理、防篡改、可信任的机制。区块链应用软件系统需对账本数据进行测试，其功能测试点主要包括如下内容：

- a) 账本历史数据可追溯功能
 - 1) 区块链应用软件系统是否可查询数据状态信息，包括如下数据的当前状态信息：
 - 账户数据、交易数据、配置数据、智能合约状态数据的当前状态信息；
 - 智能合约内可执行代码、智能合约内数据的当前状态信息。
 - 2) 区块链应用软件系统是否可查询账本数据的单个账户/所有账户的历史更新记录及交易详情（包括交易唯一标识、交易发生时间、交易哈希值、交易发起者标识、交易执行结果等）；
 - 3) 区块链应用软件系统能否根据数据对象的标识查询到该历史数据文件（包括账户配置、交易、拥有智能合约状态、账户执行智能合约等历史记录）；
 - 4) 区块链应用软件系统能否根据数据对象查询对应的交易更新记录，包括对应交易记录的发起者；
 - 5) 区块链应用软件系统能否根据时间、记录数等条件查询用户指定范围内数据更新记录（包括对账户数据、配置数据、账户拥有的智能合约状态、账户执行智能合约的历史记录）；
 - 6) 节点从异常状态恢复后，区块链应用软件系统能否正确完成历史数据溯源的查询。

- b) 数据同步功能
 - 1) 节点升级后，区块链应用软件系统能否可正确提供账本数据相关信息；
 - 2) 不同节点其数据与源节点的数据是否保持一致；
 - 3) 新节点在同步后，其数据与其他节点是否保持一致；
 - 4) 节点关闭重启或断网一段时间后，能否自动增量同步相邻节点历史数据并进行一致性校验；
 - 5) 节点是否具备与网络中的源节点进行数据同步的能力，当前源节点失效时，能否自动切换最优的源节点；
 - 6) 节点能否识别源数据节点恶意篡改同步数据，并对恶意篡改数据进行记录和提示；
 - 7) 节点能否根据账本历史记录及时检测出状态数据库数据的缺失或篡改，并进行修复；
 - 8) 节点能否通过数据同步纠正本节点的数据异常问题，保证整个网络数据的一致性。
- c) 数据归档功能
 - 1) 区块链应用软件系统能否提供账本数据归档功能，包括但不限于磁盘文件数据、数据库存储数据；是否只有对应权限的管理员才可发起归档操作；
 - 2) 区块链应用软件系统是否支持用户设置归档数据范围，包括但不限于时间、区块序号等范围限定，并完成相应的数据归档；
 - 3) 归档数据与节点本地存储的数据库中数据、数据内容一致；
 - 4) 节点在数据归档过程中，区块链应用软件系统能否继续提供系统服能；
 - 5) 节点数据归档完成后，区块链应用软件系统是否对归档的数据提供历史状态查询功能；
 - 6) 不同节点归档的数据是否存放在不同的存储设备中，防止出现集中数据丢失；
 - 7) 节点数据归档过程中，出现异常场景（如节点断电、重启、网络波动等）恢复后，能否继续完成数据归档操作；
 - 8) 区块链应用软件系统的归档数据能否恢复到在线数据库，且归档数据能否支持在线查询。
- d) 数据扩容功能
 - 1) 是否由有管理权限的用户进行扩容操作；
 - 2) 扩容中：
 - 用户交易能否正常完成，区块链网络能否正常产生区块；
 - 在异常场景恢复后，节点能否完成存储扩容，并继续正常运行；
 - 在异常场景出现扩容失败时是否具备恢复能力。
 - 3) 扩容后，账本数据文件是否具备完整性，且节点能否正常运行；
 - 4) 扩容方案是否具备平滑伸缩能力，即保障在线应用软件系统不必中断运行。

6.1.5 成员管理

区块链应用软件系统的成员管理通常包括身份管理、权限管理、数据保密、可审计功能等要素，因此其功能测试点主要包括如下：

- a) 区块链应用软件系统是否支持用户注册；
- b) 用户身份鉴别功能
 - 1) 用户身份认证过程中，区块链应用软件系统是否使用经国家密码管理部门认可的密码算法和协议；
 - 2) 区块链应用软件系统是否对用户账号使用情况进行安全性分析，包括但不限于登录时间，登录位置、访问时长等；
 - 3) 用户口令等身份认证相关凭证信息（如用户账号、口令）是否存储安全；
 - 4) 重要信息是否采用双重身份认证。
- c) 用户权限管理功能

- 1) 区块链应用软件系统的用户权限变更操作是否由身份注册机构完成或发起;
- 2) 区块链应用软件系统的用户特殊权限授权是否由身份注册机构完成授权;
- 3) 用户权限变更后
 - 区块链应用系统软件是否在不同节点间同步;
 - 区块链应用软件系统的用户是否能正常使用新权限所赋予的操作;
 - 区块链应用软件系统的用户是否不能再使用旧权限所赋予的操作。
- d) 生命周期管理功能
 - 1) 区块链应用软件系统是否提供成员全生命周期管理, 包括注册、冻结、解冻以及注销等一系列功能管理;
 - 2) 冻结状态的用户是否不能发起交易请求, 且状态是否同步到所有节点;
 - 3) 冻结的用户是否可进行解冻, 解冻后的用户能否正常发起交易, 其解冻状态是否能同步到所有节点;
 - 4) 账户是否设定使用期限; 当到达使用期限时, 账户是否被注销, 其状态是否同步到其他节点;
 - 5) 账户被注销后, 是否保留其登记信息和身份标识; 当使用注销账户的身份信息进行注册时, 是否注册失败;
 - 6) 账户被注销后, 是否无法进行交易;
 - 7) 节点异常场景恢复后, 被注销/冻结的用户是否不可发起交易。
- e) 审计功能
 - 1) 区块链应用软件系统是否可通过用户唯一标识查询成员身份信息;
 - 2) 区块链应用软件系统中注册机构是否有权查询用户所有信息;
 - 3) 不同节点查询的用户信息是否一致;
 - 4) 用户处于冻结状态时, 区块链应用软件系统是否支持可查询身份信息;
 - 5) 用户解冻后, 区块链应用软件系统是否支持可查询身份信息;
 - 6) 节点异常场景恢复后, 区块链应用软件系统查询的用户信息是否保持一致。
- f) 交易功能
 - 1) 用户登录账户向其他一个/多个账户发起交易, 能否获得交易收据, 并根据交易收据核验交易成功;
 - 2) 节点异常场景恢复后, 查询到的用户账户数据修改与交易修改是否保持一致;
 - 3) 是否自由订阅上架智能合约信息。

6.1.6 状态管理

区块链应用软件系统的状态管理主要包括区块详情查询、交易信息查询、账本状态查询等功能, 其功能测试点主要包括如下:

- a) 区块详情查询功能
 - 1) 选定区块, 区块链应用软件系统是否可查询该区块的详情 (包括区块高度、区块哈希值、前序区块哈希值、交易列表、区块时间戳等);
 - 2) 选定业务类型, 区块链应用软件系统是否可查询该业务所有区块的详情 (包括区块高度、区块哈希值、前序区块哈希值、交易列表、区块时间戳等);
 - 3) 通过区块标识, 区块链应用软件系统是否可查询指定区块的详情 (包括区块高度、区块哈希值、前序区块哈希值、交易列表、区块时间戳等);
 - 4) 节点异常场景恢复后, 区块链应用软件系统能否继续支持区块详情的查询;
 - 5) 有权限的用户是否可进行区块详情查询;

- 6) 没有权限的用户是否不可进行区块详情查询。
- b) 交易信息查询功能
 - 1) 区块链应用软件系统是否可查询交易信息（包括交易发生时间、交易哈希值、交易接受者标识、交易数据、交易发起者标识和交易所在块标识等）；
 - 2) 通过交易标识，区块链应用软件系统是否可查询该交易信息（包括交易发生时间、交易哈希值、交易接受者标识、交易数据、交易发起者标识和交易所在块标识等）；
 - 3) 选定业务类型，区块链应用软件系统是否可查询该业务上所有交易信息（包括交易发生时间、交易哈希值、交易接受者标识、交易数据、交易发起者标识和交易所在块标识等）；
 - 4) 节点异常场景恢复后，区块链应用软件系统能否继续支持区块交易信息的查询。
- c) 账本状态查询
 - 1) 通过身份账户标识，区块链应用软件系统是否可查询到指定身份账户当前状态；
 - 2) 通过身份账户标识和查询范围，区块链应用软件系统是否可查询该账户状态更新的历史记录；
 - 3) 通过身份账户标识和区块标识，区块链应用软件系统是否可查询该账户状态更新的历史记录；
 - 4) 通过智能合约标识，区块链应用软件系统是否可查询该智能合约数据的最新状态；
 - 5) 通过区块标识和智能合约标识，区块链应用软件系统是否可查询到该智能合约数据的历史状态；
 - 6) 节点异常场景恢复后，区块链应用软件系统能否继续支持账本状态查询。

6.1.7 接口管理

区块链应用软件系统的接口管理主要包括外部接口、用户接口、管理接口以及系统间接口等，其功能测试点主要包括如下：

- a) 外部接口
 - 1) 区块链应用软件系统是否提供接口调用方法说明；
 - 2) 外部接口是否设置白名单；
 - 3) 外部接口接入是否采用电子签名、数据摘要等技术手段确保数据不可篡改；
 - 4) 调用外部接口时是否采用数字证书方式保证身份真实性。
- b) 用户接口
 - 1) 区块链应用软件系统是否提供用户接口使用说明；
 - 2) 是否设置接口访问权限。
- c) 管理接口
 - 1) 区块链应用软件系统是否提供管理接口说明；
 - 2) 是否只有系统管理员可调用管理接口创建不同级别的用户，并设置访问权限。
- d) 系统间接口
 - 1) 区块链应用软件系统是否提供系统间接口功能、格式、方法、参数、返回值、使用方式、错误信息等完整说明；
 - 2) 区块链应用软件系统间接口访问是否有权限控制。

6.2 性能效率

区块链应用软件系统分别从时间特性、资源利用性、容量以及性能效率依从性四个方面来判定其基本的性能。

6.2.1 时间特性

时间特性测试点主要包括：

- a) 块信息查询：响应时间、吞吐量、事务正确率是否满足需求；
- b) 交易信息查询：响应时间、吞吐量、事务正确率是否满足需求；
- c) 交易结果查询：响应时间、吞吐量、事务正确率是否满足需求；
- d) 智能合约数据查询：响应时间、吞吐量、事务正确是否率满足需求；
- e) 历史数据查询：响应时间、吞吐量、事务正确率是否满足需求；
- f) 原生交易：响应时间、吞吐量、事务正确率是否满足需求；
- g) 智能合约调用：响应时间、吞吐量、事务正确率是否满足需求。

6.2.2 资源利用率

资源利用率测试点主要包括：

- a) 块信息查询：CPU 占用率、内存占用率、传输宽带负载以及 I/O 设备占用率是否满足需求；
- b) 交易信息查询：CPU 占用率、内存占用率、传输宽带负载以及 I/O 设备占用率是否满足需求；
- c) 交易结果查询：CPU 占用率、内存占用率、传输宽带负载以及 I/O 设备占用率是否满足需求；
- d) 智能合约数据查询：CPU 占用率、内存占用率、传输宽带负载以及 I/O 设备占用率是否满足需求；
- e) 历史数据查询：CPU 占用率、内存占用率、传输宽带负载以及 I/O 设备占用率是否满足需求；
- f) 原生交易：CPU 占用率、内存占用率、传输宽带负载以及 I/O 设备占用率是否满足需求；
- g) 智能合约调用：CPU 占用率、内存占用率、传输宽带负载以及 I/O 设备占用率是否满足需求。

6.2.3 容量

容量测试点主要包括：

- a) 块信息查询
 - 1) 在要求的负载下,单位时间内可处理最大请求数量以及可处理的最大累积事务数量是否满足需求；
 - 2) 在规定的时间内,可处理完成最大数据量是否满足需求。
- b) 交易信息查询
 - 1) 在要求的负载下,单位时间内可处理最大请求数量以及可处理的最大累积事务数量是否满足需求；
 - 2) 在规定的时间内,可处理完成最大数据量是否满足需求。
- c) 交易结果查询
 - 1) 在要求的负载下,单位时间内可处理最大请求数量以及可处理的最大累积事务数量是否满足需求；
 - 2) 在规定的时间内,可处理完成最大数据量是否满足需求。
- d) 智能合约数据查询
 - 1) 在要求的负载下,单位时间内可处理最大请求数量以及可处理的最大累积事务数量是否满足需求；
 - 2) 在规定的时间内,可处理完成最大数据量是否满足需求；
- e) 历史数据查询
 - 1) 在要求的负载下,单位时间内可处理最大请求数量以及可处理的最大累积事务数量是否满足需求；

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/865322012203012111>