ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0193—2020

区块链技术金融应用 评估规则

Financial application of blockchain technology—Evaluation rules

2020－07－10 发布　　2020－07－10 实施

中国人民银行　　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 3
5 总则 3
5.1 评估目标 3
5.2 启动条件 3
5.3 评估方法 3
5.4 评估判定准则 3
6 基本要求评估 4
6.1 账本技术 4
6.2 共识协议 17
6.3 智能合约 20
6.4 节点通信 24
6.5 事件分发 27
6.6 密钥管理 29
6.7 状态管理 32
6.8 成员管理 36
6.9 交易系统 43
6.10 接口管理 47
7 性能评估 51
7.1 交易吞吐率 51
7.2 查询吞吐率 52
7.3 交易同步性能 53
7.4 部署效率 55
7.5 账本数据增长速率 55
8 安全性评估 56
8.1 基础硬件 56
8.2 基础软件 59
8.3 密码算法 64
8.4 节点通信 67
8.5 账本数据 69
8.6 共识协议 76

8.7 智能合约 79
8.8 身份管理 81
8.9 隐私保护 85
8.10 监管支撑 87
8.11 安全运维 89
8.12 安全治理 92

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行科技司、中国人民银行数字货币研究所、中国金融电子化公司、中国银联股份有限公司、中钞区块链技术研究院、国家开发银行、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、交通银行股份有限公司、招商银行股份有限公司、上海浦东发展银行股份有限公司、中信银行股份有限公司、兴业银行股份有限公司、中国民生银行股份有限公司、浙江网商银行股份有限公司、深圳前海微众银行股份有限公司、光大科技有限公司、中国平安保险（集团）股份有限公司、泰康保险集团股份有限公司、华泰证券股份有限公司、深圳市腾讯计算机系统有限公司、京东数字科技控股股份有限公司、百度在线网络技术（北京）有限公司、浙江蚂蚁小微金融服务集团股份有限公司、华为技术有限公司、龙盈智达（北京）科技有限公司、杭州溪塔科技有限公司、杭州趣链科技有限公司、北京轻信科技有限公司、杭州云象网络技术有限公司、清华大学、北京大学、中国科学院计算技术研究所、中国人民大学金融科技研究所、中国支付清算协会、北京中金国盛认证有限公司、北京银联金卡科技有限公司。

区块链技术金融应用 评估规则

1 范围

本标准规定了区块链技术金融应用的具体实现要求、评估方法、判定准则等。

本标准适用于金融机构开展区块链技术金融应用的产品设计、软件开发、系统评估。

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 5271.18—2008 信息技术词汇

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 32915 信息安全技术 二元序列随机性检测方法

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0184—2020 金融分布式账本技术安全规范

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

一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、防篡改、防抵赖的技术体系。

注：典型的区块链是以块链结构实现数据存储的。

3.2

区块 block

区块链中存储数据的单元。

注：由区块头和区块体组成。

3.3

共识节点 consensus node

负责账本数据一致性的节点。

[JR/T 0184—2020,定义 3.24]

3.4

记账节点 accounting node

负责账本数据完整性的节点。
[JR/T 0184—2020, 定义 3.25]

3.5

用户 user

参与到区块链上实际责任主体的基本单位。

3.6

数据变更 data changes

对区块链上单个或多个账户的数据进行变更的操作。
示例：智能合约的部署、合同状态的变更、配置参数的修改等。

3.7

原子性 atomicity

智能合约在执行过程中发生错误，会被回滚到智能合约开始前的状态。
[JR/T 0184—2020, 定义3.36]

3.8

交易 transaction

区块链上的一次原子性账本数据状态变更及其过程和结果记录。

3.9

资产 asset

能够在区块链上发行、流通、存储、交易，用于完成支付清算业务的权益。

3.10

节点授权 node authorization

在区块链系统中决定一个提出请求的节点（客体）是否有权限访问资源（主体）的动作。

3.11

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]

3.12

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。
[JR/T 0184—2020, 定义 3.17]

3.13

智能合约 smart contract

一种旨在以信息化方式传播、验证或执行合同的计算机协议，其在分布式账本上体现为可自动执行的计算机程序。

[JR/T 0184—2020,定义 3.20]

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）

TEE：可信执行环境（Trusted Execution Environment）

CA：数字证书认证（Certificate Authority）

5 总则

5.1 评估目标

在区块链技术金融应用系统版本确定的基础上，对区块链金融应用的基本要求、性能、安全性进行评估，客观、公正评价系统是否能够保障区块链金融设施与应用的安全稳定运行。

5.2 启动条件

启动条件具体包括：

a) 提交的系统（或可执行文件）被测版本应与生产版本一致。

b) 提交的系统应已完成内部测试。

c) 系统需求说明书、系统设计说明书、用户手册（包括但不限于运维手册、使用手册）、产品手册（包括但不限于组件列表、特性指标、系统架构）等相关文档应准备完毕。

d) 最小硬件要求：机构应披露其区块链系统在满足共识有效性的要求下，正常运行的最小硬件资源，包含硬件设备和网络要求，需验证最小硬件环境下功能、可靠性的完备。

e) 评估环境应准备完毕，具体包括：

1) 评估环境应与生产环境一致或者基本一致，基本要求、性能、安全性宜在生产环境下进行。

2) 系统被测版本及其他相关外围系统和设备应已完成部署并配置正确。

3) 用于基本要求和性能评估的基础数据应准备完毕。

4) 评估用设备应准备到位，系统及软件安装完毕。

5) 评估环境网络应配置正确，连接通畅，可以满足评估需求。

5.3 评估方法

评估方法及说明如下：

a) 查阅材料：查阅审计报告、自查报告、外部评估报告、设计文档、开发文档、用户文档、管理文档、产品检测报告等相关材料。

b) 查看系统：查看系统日志、配置文件、参数设置、产品版本、网络配置等。

c) 访谈人员：与被测系统或产品有关人员进行交流、讨论等活动，获取相关证据，了解有关信息。

d) 测试系统：利用专业工具，通过对目标系统的扫描、探测等操作，使其产生特定的响应等活动，通过分析响应结果，获取证据以证明信息系统的基本要求、性能、安全性是否得以有效实施。

5.4 评估判定准则

5.4.1 问题等级分类

5.4.1.1 严重性问题

严重性问题判定原则如下：

a) 与相关法律法规、标准规范有明显冲突。

b) 不满足本标准中相关要求，造成：

1) 无法满足系统基本运行和安全需求的情况。

2) 存在重大安全风险，会对客户利益造成严重损害的情况。

3) 不能满足监管支撑要求，运营活动无法受到有效监管的情况。

5.4.1.2 一般性问题

一般性问题判定原则如下：

a) 不满足本标准中相关要求，造成：

1) 局部功能无法正常使用，但不影响系统整体流程的实现。

2) 存在安全风险，会对客户利益造成直接或潜在的损害。

3) 对监管支撑存在缺陷，不利于管理部门合法监管工作的开展。

5.4.1.3 建议性问题

建议性问题判定原则如下：

a) 不满足本标准中相关要求，造成：

1) 功能能够正常使用，但系统易用性差。

2) 存在安全风险，但不会对客户利益造成直接或潜在的损害。

5.4.2 评估结果判定原则

评估结果判定原则如下：

a) 符合：在评估过程中，未发现问题或仅发现建议性问题，该评估项的评估结果判定为“符合”。

b) 不符合：在评估过程中，发现严重性问题和一般性问题，该评估项的评估结果判定为“不符合”。

c) 不适用：评估过程中，根据系统声明及各评估项中适用对象的适用性，不属于适用对象的评估项可判定为“不适用”。

6 基本要求评估

6.1 账本技术

6.1.1 数据存储方式

数据存储方式评估内容见表1。

表1 数据存储方式评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	宜兼容一种以上的数据库类型和版本	1.查阅材料 2.查看系统	1.设计文档对支持的不同类型数据库有规划和设计，支持数据库类型不少于2种，每类数据库至少支持最新发布的3个版本。 2.设计文档为开发人员提供不同类型的数据库接口API，并与设计文档支持的数据库类型和版本一致。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			3.系统配置文件中不同类型数据库的配置参数与设计文档一致。 4.系统中网络和主机访问控制策略支持所用类型数据库的端口。	
2	应选用经过评测的主流数据库版本	1.查阅材料 2.查看系统	1.设计文档使用的数据库为主流的商用或开源产品。 2.系统数据库产品的提供方公开或提供产品的权威第三方测评结果。 3.设计文档为开发人员提供的数据库接口API与设计文档支持的数据库一致。 4.系统配置文件中数据库的配置参数与设计文档一致。	金融业务系统、科技产品
3	应正确读写支持的数据库	测试系统	1.系统根据设计文档的数据库接口API向数据库写入数据后，使用该数据库提供的原生工具或第三方工具能够读出数据。 2.系统使用该数据库提供的原生工具或第三方工具按照设计文档的数据结构写入数据后，通过数据库接口API可读出数据。	金融业务系统、科技产品
4	应根据数据对象的类别分别存储、管理、操作账户数据、交易数据、配置数据等	1.查阅材料 2.测试系统	1.设计文档根据数据对象的类别规划独立存储，账户数据、交易数据、配置数据等数据分别管理、操作。 2.设计文档开发人员提供不同类型数据的访问API，并与设计文档一致。 3.系统根据设计文档提供的API写入、读取数据，不同的API读写功能正确且读写的数据对象类型不同。 4.系统使用第三方工具访问数据库，不同数据对象类型分别存储。	金融业务系统、科技产品
5	应具备高可靠性，能应对节点断电、重启、网络波动等异常场景	测试系统	系统在断电、节点重启、网络故障等异常场景恢复后存储数据能够正常读写。	金融业务系统、科技产品
6	应实现存储空间的监控和预警	1.查阅材料 2.测试系统	1.设计文档包含对数据库空间监控、报警的规划和设计。 2.使用手册包含空间不足的触发条件、报警内容、处理步骤。 3.系统在可用空间触发报警条件时发出预警。 4.系统发出预警后，按照使用手册的应急步骤进行处理，空间不足的情况消失。	金融业务系统、科技产品
7	应根据相应安全级别要求重置数据库	1.访谈人员 2.测试系统	1.管理员提供的密码足够复杂，符合金融信息系统对密码复杂度和长度的要求，且能够正常	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	的默认访问密码		访问数据库。 2.系统在使用数据库默认密码和常见密码访问数据库时，数据库能够拒绝访问。	技产品

6.1.2 账本结构

账本结构中的数据文件评估内容见表2。

表2 数据文件评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具有防篡改性	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含明确的数据防篡改策略、手段及详细说明。 2.设计文档包含开发人员提供校验数据未被篡改的接口。 3.系统区块信息中能够查到数据防篡改的哈希值等信息。 4.系统能够检测出修改的数据文件。 5.系统能够记录操作账本数据的日志，可供监管审计。 6.系统账本监控程序能够自动检测账本数据是否已篡改。	金融业务系统、科技产品
2	应具备校验完整性的功能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含数据完整性校验的说明。 2.系统提供完整性校验功能，提示数据完整性被破坏并拒绝区块新增。 3.系统提供监控手段定位账本数据的不完整。 4.系统在数据完整性被破坏的情况下，能够快速提示被破坏完整性的数据文件。	金融业务系统、科技产品
3	区块头应包含交易的梅克尔树根信息及状态数据的梅克尔树根信息	1.查阅材料 2.查看系统	1.设计文档包含区块头信息，说明了交易数据和状态数据的排序方法以及梅克尔树根的生成方式。 2.系统具有查看区块头信息的接口。 3.系统具备检测头部信息被修改的能力。	金融业务系统、科技产品

6.1.3 历史数据可追溯

若支持账本历史数据管理功能，历史数据管理评估内容见表3。

表3 历史数据管理评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应能正确查询到账本数据的当前状态信息	1.查阅材料 2.查看系统	1.使用文档具有查询账本数据当前状态信息功能的使用说明。	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
			2.系统能查询到账户数据、交易数据、配置数据、智能合约状态数据的当前状态信息。 3.系统能查询到指定智能合约内可执行代码的当前状态以及智能合约内数据的当前状态信息。	技产品
2	应能正确查询到账本数据的所有历史更新记录及交易详情	1.查阅材料 2.查看系统	1.使用文档具有查询账本数据所有历史更新记录及交易详情功能的使用说明。 2.系统能查询到所有账户数据、配置数据、智能合约状态数据、智能合约内代码和数据变更的历史更新记录以及对应的交易更新记录。 3.系统能查询到交易记录的详情，包括但不限于以下信息：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。若该交易为智能合约操作，包含智能合约执行反馈事件的信息。	金融业务系统、科技产品
3	应能正确并独立地查询到账本数据中某个账户的所有历史更新记录及交易详情	1.查阅材料 2.查看系统	1.使用文档具有查询账本数据中某个账户的所有历史更新记录及交易详情的使用说明。 2.系统能通过身份账户标识查询到某个账户的所有交易更新记录，包括账户数据、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。 3.系统能查询到交易记录的详情，包括但不限于以下信息：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；若该交易为智能合约操作，包含智能合约执行反馈事件的信息。	金融业务系统、科技产品
4	应能根据数据对象的唯一标识查询到该历史数据文件	1.查阅材料 2.查看系统	1.使用文档具有根据数据对象的唯一标识查询历史数据文件功能的使用说明。 2.系统能根据身份账户标识查询该账户的账户配置、交易、拥有智能合约状态、账户执行智能合约等历史记录。 3.系统能根据交易唯一标识查询该交易的历史交易详情。 4.系统能根据区块唯一标识查询该区块详情。	金融业务系统、科技产品
5	应能对数据来源和变更的操作者身份进行追溯	1.查阅材料 2.查看系统	1.使用文档具有对数据来源和变更的操作者身份进行追溯功能的使用说明。 2.系统能根据数据对象查询对应的交易更新记录。 3.系统能查询到对应交易记录的发起者。	金融业务系统、科技产品
6	应能根据时间、记录数等特征条件正常查	1.查阅材料 2.查看系统	1.使用文档具有根据时间、记录数等特征条件查询用户指定范围内数据更新记录功能的使	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	询到用户指定范围内数据更新记录		用说明。 2.系统能通过特定的条件查询到某个账户的所有交易更新记录，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。 3.系统能查询到交易记录的详情。	技产品
7	应能正确查询到账本数据状态变更记录所在区块文件的唯一标识和时间戳	1.查阅材料 2.查看系统	1.使用文档具有查询账本数据状态变更记录所在区块文件的唯一标识和时间戳功能的使用说明。 2.系统能根据交易唯一标识查询到所在区块的区块唯一标识。 3.系统能根据区块唯一标识查询到区块详细信息，包括但不限于区块高度、区块哈希值、前序区块哈希值、交易列表、区块时间戳。	金融业务系统、科技产品
8	应能判别对账本数据状态变更记录的先后顺序	1.查阅材料 2.查看系统	1.使用文档具有判别账本数据状态变更记录先后顺序功能的使用说明。 2.系统能根据数据对象查询对应的交易更新记录。 3.系统能查询到交易记录的详情，包括但不限于交易唯一标识、交易发生时间、交易哈希值、交易发起者标识、交易执行结果。 4.系统对于交易记录查询结果支持自动或手动根据交易发生时间或其他属性进行排序。	金融业务系统、科技产品
9	可支持通过账本查看功能对底层存储进行查询	1.查阅材料 2.查看系统	1.使用文档具有对底层存储进行查询的使用说明。 2.系统可通过账本查看功能查询到账本底层区块、交易、智能合约元数据、数据存储结构（如梅克尔树）。 3.系统可通过智能合约数据存储形式（如KV）查询智能合约内的数据集。 4.系统中智能合约数据可映射或导出到关系型数据库，允许通过SQL结构化查询的方式查询智能合约内的数据集。	金融业务系统、科技产品
10	应保证节点从异常状态恢复后，仍能够正确完成历史数据溯源	1.查阅材料 2.查看系统	1.设计文档中具有系统异常状态恢复后，要求节点数据最终一致的说明。 2.系统在节点异常状态恢复后，能够正确完成历史数据溯源的查询。 3.系统在异常状态恢复后，从各节点都能够正确完成历史数据溯源的查询。	金融业务系统、科技产品
11	应具备前向兼容性，在节点版本升级后，	1.查阅材料 2.查看系统	1.设计文档中具有系统节点版本升级后，要求节点数据最终一致的说明。	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	能够正确读取账本数据		2.系统在节点版本升级后，能够正确读取账本数据。 3.系统在节点版本升级后，从各节点都能够正确读取账本数据。	技产品

6.1.4 数据同步

数据同步评估内容见表4。

表4 数据同步评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保持需要同步数据的节点与源节点的数据一致	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含节点数据广播功能的方法说明，同时包含保证同步数据一致性的手段说明。 2.设计文档包含数据广播、查询相邻节点、查询当前区块数、获取某个区块数据等的接口说明，包括功能、格式、方法、参数、返回值、使用方式等。 3.系统能够通过登录不同节点观察数据同步情况，并根据区块头信息以及结合数据完整性的保证机制，判断节点间数据同步情况。 4.系统能够通过连接原始节点进行测试交易，并检查原始节点和不与原始节点直接相连的其他节点，确保两个节点保持一致。 5.系统数据同步机制符合一致性标准和规范。 6.系统具备监控手段自动检测节点是否符合数据一致性要求。 7.系统具备查询到所有节点的数据同步情况，如已同步节点数、节点同步进度。	金融业务系统、科技产品
2	应保持新增节点在同步所需历史数据之后与其他节点数据一致	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含新增节点数据同步方法的说明。 2.设计文档包含查询相邻节点、查询当前区块数、获取某个区块数据等的接口说明，包括功能、格式、方法、参数、返回值、使用方式等。 3.系统包含新增节点获取到老节点地址等信息的配置。 4.系统能够通过登录新加入节点观察数据同步情况，并通过比较新旧节点区块头信息，以及结合数据完整性的保证机制，判断节点间数据同步情况。 5.系统能够通过测试手段检验新节点数据同	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			步是否完成，数据是否一致的能力。 6.系统新增数据节点数据同步完成后，自动数据校验一致性机制能够判断数据异常情况，并给出提示。	
3	应保持单节点在重启并同步缺失增量数据后与其他节点的数据一致	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含节点间数据增量同步方法的说明及日志记录要求。 2.设计文档包含查询相邻节点、查询当前区块数、获取某个区块数据等的接口说明，包括功能、格式、方法、参数、返回值、使用方式等。 3.系统能够通过登录节点观察数据同步情况，并通过比较节点区块头信息以及结合数据完整性的保证机制，判断节点间数据同步情况。 4.系统在一个节点关闭重启或断开网络一段时间后，可自动增量同步相邻节点历史数据并进行一致性校验。 5.系统包含人工手段的应急措施确保重启后的节点数据一致性。 6.系统能够记录增量数据同步过程中的故障日志，并与设计文档一致。	金融业务系统、科技产品
4	应支持单节点在同步数据过程中可动态切换源数据节点	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含源节点检测、连接、切换的方法说明。 2.设计文档包含查询相邻源节点、查询当前区块数、获取某个区块数据等的接口说明，包括功能、格式、方法、参数、返回值、使用方式等。 3.系统节点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，能够自动切换最优的源节点。 4.系统具备通过人工手段切换数据源能力，确保单个节点能够完成数据同步。 5.系统中同步的源节点断开网络后，可自动连接其他相邻节点，继续进行同步的能力。	金融业务系统、科技产品
5	应确保在多节点网络中，节点互相同步历史数据的一致性，避免同步错乱	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含保证数据连续一致性的手段说明。 2.设计文档包含校验数据连续一致性的接口说明。 3.系统能够通过登录不同节点比较数据连续性。 4.系统的数据连续一致性实现方式与设计文档一致。 5.系统在数据同步过程中，源节点新增数据能	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			够被同步到目标节点，目标节点能够校验源节点数据的完整性。 6.系统具备历史数据自动校验的能力，能够对错乱数据进行系统自动恢复。 7.系统具备完善的系统日志功能。	
6	应满足在多节点网络中，节点同步历史数据达到一致状态的时效性	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中能够针对应用典型和异常场景下的数据量，说明达到共识要求所需节点间同步一致的时效性要求。 2.系统包含节点历史数据同步状态进展查询功能以及节点间同步一致性核验功能。 3.系统在以下测试场景下满足数据同步时效性要求：典型应用场景下数据定量的单节点或多节点的同步一致性与时效性测试；异常场景下数据定量的单节点或多节点的同步一致性与时效性测试。	金融业务系统、科技产品
7	节点在同步数据过程中出现异常场景，异常场景恢复后能够从异常场景前已同步的数据文件开始继续同步剩余的区块文件	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含针对节点同步区块过程中断网、断电、网络波动等异常场景恢复后，区块数据能够继续断点续传的功能说明。 2.系统区块同步过程中具有异常场景下自动发现与提示功能、自动重连功能、区块断点续传后数据一致性校验功能。 3.系统具备完善的系统日志功能。 4.系统能够通过多节点网络下区块同步断网、断电、网络波动等各类异常场景的测试。	金融业务系统、科技产品
8	应确保节点在同步数据过程中能够识别出源节点数据被恶意篡改	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含对应源数据节点恶意篡改同步数据的核对算法或共识算法逻辑，防止源数据节点恶意篡改生效的说明。 2.系统具有识别源数据节点恶意篡改同步数据的功能，并对恶意篡改数据记录和提示。 3.系统能够通过对单源数据节点或多源数据节点的恶意篡改的测试。	金融业务系统、科技产品
9	应确保状态数据可重建，并根据交易序列重建状态数据	1.查阅材料 2.查看系统 3.访谈人员	1.设计文档包含支持底层数据结构满足状态数据可重建，并可根据交易序列重建状态数据的能力详细说明。 2.系统能够实现状态数据根据交易序列进行重建，并与设计文档一致。 3.系统节点能够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。	金融业务系统、科技产品
10	节点应可通过数据同步纠正本节点的数据	1.查阅材料	1.设计文档具有保证节点数据正常、网络一致性的设计说明，具有单节点数据异常纠正机制	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	异常问题，保证整个网络数据的一致性	2.查看系统 3.测试系统	的说明。 2.设计文档包含针对实际业务场景实现数据最终一致性、避免业务风险的说明。 3.系统具备通过自检程序校验区块链系统各节点账本数据的正确性、完整性和一致性；系统在功能设计上记录显示本节点前期数据异常以及同步一致后正常数据差异相关交易。 4.系统在本节点数据异常时能够恢复，单节点数据异常时整体业务运行不受影响。	技产品

6.1.5 数据归档

数据归档功能评估内容见表5。

表5 数据归档评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应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	1.查阅材料 2.查看系统	1.设计文档对支持账本数据归档功能有规划和设计，归档方式可使用磁盘文件、数据库存储等可持久化的存储方式。 2.系统配置文件中有归档功能的相关配置参数，并与设计文档一致。 3.系统进行归档操作后，在设定归档数据存放的磁盘、数据库中有对应的归档数据。	金融业务系统、科技产品
2	应由相应管理员权限的用户发起归档操作	测试系统	1.系统由非管理员权限的用户发起归档操作，在设置的归档数据存放的磁盘、数据库中不出现有对应的归档数据。 2.系统由管理员权限的用户发起归档操作，在设置的归档数据存放的磁盘、数据库中有对应的归档数据。	金融业务系统、科技产品
3	应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，完成相应的数据归档	查看系统	系统按使用说明设置归档数据归档范围，成功进行归档操作后的归档数据符合所设定的范围。	金融业务系统、科技产品
4	归档数据与节点本地存储的数据应具备数据完整性，不缺失账本数据	查看系统	系统归档的数据与归档之前本地存储的数据库中数目、数据内容一致。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
5	数据归档的存储介质应具备高可靠性	查看系统	系统归档数据的存储介质在具备高可靠性的设施中，设施具备容灾、服务宕机自动恢复、数据容错、数据备份和数据恢复等能力。	金融业务系统、科技产品
6	节点在数据归档过程中，应能够继续提供系统服务，可暂时停止历史状态查询功能	查看系统	系统执行节点归档功能的过程中，新增交易数据处理能正确进行，新增交易数据能被正确查询。	金融业务系统、科技产品
7	节点数据归档完成后，应对归档的数据支持历史状态查询功能	查看系统	系统节点归档完成后，历史数据能查询。	金融业务系统、科技产品
8	不同节点归档的数据应存放在不同的存储设备中，防止出现集中数据丢失	查看系统	系统中两个节点归档操作执行完成后，两个节点的归档存储位置在不同的存储设备中。	金融业务系统、科技产品
9	节点数据归档过程中，出现节点断电、重启、网络波动等异常场景恢复后，节点宜继续完成数据归档操作	查看系统	系统在归档过程中，节点恢复后继续正确执行归档处理。	金融业务系统、科技产品
10	宜支持归档数据恢复还原功能，能够将归档数据全部或部分恢复还原到在线数据库	查看系统	系统归档数据可恢复到在线数据库，归档数据能在线查询。	金融业务系统、科技产品

6.1.6 数据扩容

数据扩容评估内容见表 6。

表6 数据扩容评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供存储的扩容技术和方案	查阅材料	扩容方案采取可行性及安全性兼具的主流成熟技术栈，包括但不限于磁盘空间和数据库扩容技术。	金融业务系统、科技产品
2	应在数据扩容后保证性能稳定	1.查阅材料 2.测试系统	1.扩容方案中提供数据增长趋势说明。 2.系统数据扩容实施完成后，系统性能稳定。	金融业务系统、科技

序号	实现要求	评估方法	结果判定	适用对象
				产品
3	应由具有管理权限的用户操作触发扩容操作	1.查阅材料 2.查看系统	1.扩容方案中详细说明操作人员名单及职责，符合权限最小原则。 2.系统保留扩容实施期间的所有操作日志，确保只有具备相关权限的人员进行操作。	金融业务系统、科技产品
4	扩容完成后，账本数据文件应具备完整性，且节点能够正常运行	1.查阅材料 2.测试系统	1.扩容方案中具有保证账本数据文件完整性的说明。 2.系统数据扩容完成后，节点能正常运行且账本文件与其他节点所存储账本文件一致。	金融业务系统、科技产品
5	扩容过程中，应确保用户发送交易、同步区块文件等操作不会导致节点账本数据文件异常	1.查阅材料 2.测试系统	1.扩容方案中说明了扩容过程中保障用户发送交易、同步区块文件等操作不会导致节点账本数据文件异常的方法。 2.系统扩容实施过程中，用户交易能正常完成，区块链网络能正常产生区块。	金融业务系统、科技产品
6	扩容过程中，节点在异常场景恢复后应能完成存储扩容并具备正常运行能力	1.查阅材料 2.查看系统 3.测试系统	1.扩容方案中说明了节点断电、重启、网络波动等异常场景下的处理机制。 2.系统在异常场景恢复后，节点能够完成存储扩容，并继续正常运行。 3.系统在异常场景出现扩容失败时具备恢复能力。	金融业务系统、科技产品
7	扩容方案应具备平滑伸缩能力，保障在线系统不必中断运行	1.查阅材料 2.查看系统 3.测试系统	1.扩容方案中说明了使用平滑伸缩能力保障在线系统正常运行的方法。 2.当采取分片技术进行平滑扩容时，系统在特定高度扩容前后，分片数据处理逻辑一致。 3.系统共识算法的可回滚性对扩容操作无影响。	金融业务系统、科技产品

6.1.7 数据跨链功能

若支持账本数据跨链功能，数据跨链功能评估内容见表7。

表7 数据跨链功能评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证跨链交易在不同链上的执行结果一致	1.查阅材料 2.测试系统	1.设计文档对跨链功能的设计具有维护交易一致性的措施。 2.使用文档对跨链功能有详细、明确的操作步骤。 3.系统能正确完成跨链交易，不同链上执行结果一致。	金融业务系统、科技产品
2	跨链交易对不同链上	1.查阅材料	1.设计文档对跨链功能的设计涉及对账本状	金融业务

序号	实现要求	评估方法	结果判定	适用对象
	状态数据的修改应正确更新到账本状态中	2.测试系统	态的修改。 2.使用说明文档对跨链功能有详细、明确的操作步骤。 3.系统按照说明文档的操作步骤能完成跨链交易。 4.系统完成跨链交易后，账本状态产生变化且符合业务处理逻辑。	系统、科技产品
3	应在一次跨链交易中支持多条链之间实现数据修改	1.查阅材料 2.测试系统	1.设计文档对跨链功能的设计支持多条链的情形。 2.使用说明文档对跨链功能有详细、明确的操作步骤。 3.系统按照说明文档的操作步骤完成一笔跨链交易后，多条相关链的数据发生变化且变化符合业务处理逻辑。	金融业务系统、科技产品
4	应由参与的多个账户协商一致才能发起并完成跨链交易	1.查阅材料 2.测试系统	1.设计文档对跨链功能的设计中明确了跨链前须达成协商一致的要求。 2.使用说明文档对跨链功能有详细、明确的操作步骤。 3.系统按照说明文档的操作步骤，所有账户协商一致后能够成功发起跨链交易。 4.系统按照说明文档的操作步骤，当仅有部分用户发起跨链交易时，交易显示失败并提示交易失败的原因。	金融业务系统、科技产品
5	应基于当前链的账本状态单独验证跨链交易	测试系统	1.系统通过非跨链交易修改链上账本的特定账户的数据，发起跨链交易，当前区块链交易验证为不通过。 2.系统切换另外一个账户，在另外一条链上通过非跨链交易修改其链上账本中此账户的数据，发起跨链交易，当前区块链交易验证为通过。	金融业务系统、科技产品
6	应在跨链交易中正确应对节点断电、重启、网络波动等异常场景	测试系统	1.系统在断电、节点重启、网络故障等异常场景恢复后，各条链上的交易执行结果一致且符合业务处理逻辑。 2.系统在异常场景恢复后，各条链上的状态数据一致且符合业务处理逻辑。	金融业务系统、科技产品
7	应在跨链交易中满足事务完整性	1.查阅材料 2.测试系统	1.设计文档对跨链功能的设计有跨链事务一致性的处理说明。 2.系统在切断两条链的网络联接情况下，跨链交易显示超时，当前链的处理回滚到交易发起前的状态。 3.系统通过非跨链交易修改另外一条链的特	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			定账户的账本数据，发起跨链交易，另外一条链将交易验证为不通过，当前链虽然将交易验证为通过，也会回滚此交易的处理。	

6.1.8 数据分片功能

若支持数据分片技术，数据分片功能评估内容见表 8。

表8 数据分片功能评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	系统分片技术方案应能够有效提升系统交易处理性能	1.查阅材料 2.测试系统	1.分片技术方案采用目前主流成熟的技术栈，实施前进行了相关评审。 2.说明文档提供分片技术提升系统处理性能的相关说明。 3.系统分片后交易处理TPS平均值和峰值有显著的提升。	金融业务系统、科技产品
2	应支持多种及用户自定义的数据分片策略，实现账本数据存储到不同片区	1.查阅材料 2.测试系统	1.技术方案支持多种分片策略，包括但不限于网络分片、交易分片及状态分片，提供用户自定义的分片策略，并提供不同分片策略的配置方案及说明。 2.系统在分片后能够把不同的账本数据存储在不同的片区中，并保证数据的完整性。	金融业务系统、科技产品
3	应支持跨数据片交易的一致性及交易的执行结果在不同数据片上保持一致性	1.查阅材料 2.测试系统	1.设计文档具有保证系统跨数据片交易的执行结果一致性的说明。 2.系统分片后进行跨数据片的交易，不同数据片的交易执行结果一致。	金融业务系统、科技产品
4	系统跨链交易对不同数据片上状态数据的修改应能正确更新到账本状态中	1.查阅材料 2.测试系统	1.设计文档说明了系统在跨链交易时，对不同数据片状态数据修改能正确更新到账本状态中。 2.系统分片后进行跨数据片交易，不同数据片的账本状态能够正确同步更新。	金融业务系统、科技产品
5	系统中跨数据片的一条交易中应支持多条数据片相互之间实现数据修改，并保证结果一致性	1.查阅材料 2.查看系统 3.测试系统	1.设计文档说明了跨数据片的一条交易中支持多条数据片相互之间实现数据修改，并保证最终交易数据结果一致性。 2.系统分片后能够在不同的数据片之间，实现同一条交易数据的修改。 3.系统分片后对同一条交易数据修改，每个分片的交易数据结果和账本数据结果一致。	金融业务系统、科技产品
6	应保证跨数据片交易中，每个数据片单独验证结果具有独立性	1.查阅材料 2.测试系统	1.设计文档说明了跨数据片交易下，每个数据片上单独验证结果由该数据片的账本状态决定而不受其他数据片上验证结果影响。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			2.系统发送多个分片的跨数据片交易，每个数据片的单独验证结果不受其他数据片影响。	
7	应保证跨数据片交易过程中，出现节点断电、重启、网络波动等异常场景恢复后，各数据片上节点的交易执行结果一致并且交易数据更新状态一致	1.查阅材料 2.测试系统	1.设计文档说明了系统在断电、重启、网络波动等异常场景恢复后，各分片交易数据以及账本交易数据不受影响。 2.系统异常场景恢复后各分片上的节点数据交易结果以及更新后的状态数据结果，与系统无异常场景下结果一致。	金融业务系统、科技产品

6.2 共识协议

6.2.1 共识算法

共识算法评估内容见表9。

表9 共识算法评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应支持声明的共识算法	1.查阅材料 2.测试系统	1.设计文档中包含系统支持的共识算法说明。 2.系统基于声明的所有不同的共识算法，均能实现预期功能，系统正常运行。	金融业务系统、科技产品
2	应在节点在线、节点离线、网络规模调整等情况下，切换共识机制能达成全网新的共识	1.查阅材料 2.测试系统	1.设计文档中包含共识算法切换方法及条件相关说明。 2.系统切换共识机制后，节点在线、节点离线、网络规模调整等情况下，均能达成全网新的共识，系统正常运行。	金融业务系统、科技产品

6.2.2 一致性

共识算法一致性评估内容见表10。

表10 共识算法一致性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保持每个节点更新账本状态写操作的一致性	1.查阅材料 2.测试系统	1.设计文档中包含账本更新操作相关说明。 2.系统任意节点发起交易更新账本后，系统交易（共识成功或共识失败）更新操作记录中，针对正常交易与异常交易的写操作结果一致。	金融业务系统、科技产品
2	应保证每个节点账本的最终状态一致	1.查看文档 2.测试系统	1.设计文档中包含共识算法一致性相关说明。 2.任意节点发起交易更新账本后，各节点最终	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	性		状态一致。	技产品
3	共识过程中出现节点断电、重启、网络波动等异常场景并恢复后，所有节点交易执行的结果最终一致	1.查阅材料 2.测试系统	1.设计文档中包含节点恢复、数据恢复机制相关说明。 2.系统在任意数量节点出现异常场景下，各节点恢复后交易状态一致。	金融业务系统、科技产品
4	同样的交易在同一或不同节点多次运行，应保证执行结果的唯一确定性	1.查阅材料 2.测试系统	1.设计文档中包含交易执行机制相关说明。 2.系统选取任意节点发起相同交易，各个节点交易执行结果唯一且一致。	金融业务系统、科技产品
5	应保证交易在每个节点执行时具备可终止性	1.查阅材料 2.测试系统	1.设计文档中包含交易执行机制相关说明。 2.系统选取某个节点发起交易用例，各个节点交易执行可终止。	金融业务系统、科技产品

6.2.3 共识节点数量

共识算法若限制节点数量，共识节点数量评估内容见表11。

表11 节点数量评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应规定共识算法最少需要的参与节点数量	1.查阅材料 2.测试系统	1.设计文档包含共识算法最少需要参与的节点数量的具体规定。 2.系统选取最少共识节点数量进行测试，具备正确达成共识的能力。	金融业务系统、科技产品
2	应规定最多支持的共识节点数量	1.查阅材料 2.测试系统	1.设计文档包含对最多支持的共识节点数量的描述。 2.系统在最多共识节点数量的情况下具备正确共识的能力。	金融业务系统、科技产品

6.2.4 容错阈值

共识机制容错阈值评估内容见表12。

表12 容错阈值评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供共识算法的容错阈值	查阅材料	设计文档中申明了共识算法可接受的故障或恶意共识节点的比例。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
2	应在不超过最大阈值恶意节点下,能正确达成共识	测试系统	系统在不超过最大容错阈值的共识节点离线时，能正确达成共识。	金融业务系统、科技产品
3	应具备拜占庭容错能力	测试系统	系统在不超过最大容错阈值的共识节点发送错误的共识投票消息时，能正确达成共识。	金融业务系统、科技产品
4	应在超过最大阈值恶意节点情况下,无法正确达成共识	测试系统	1.系统在超过最大阈值的共识节点离线时，无法达成共识。 2.系统在超过最大阈值的共识节点发送错误消息时，无法达成共识。	金融业务系统、科技产品

6.2.5 可靠性

共识算法的可靠性评估内容见表 13。

表13 共识算法可靠性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	共识算法应具备抗攻击和识别恶意节点的能力	1.查阅材料 2.测试系统	1.设计文档对共识算法的抗攻击能力有规划和设计，支持抗DDoS攻击、重放攻击、识别恶意节点的能力。 2.系统共识算法经测试具备抗 DDoS 攻击、重放攻击、识别恶意节点的能力。	金融业务系统、科技产品
2	节点从异常场景恢复后应保证数据正常恢复、数据不丢失及正常参与共识流程	1.查阅材料 2.测试系统	1.设计文档对断电、重启、网络波动等异常场景恢复后节点数据正常恢复且不丢失、节点能参与进行正确的共识流程有规划和设计。 2.节点从异常场景恢复后，节点的数据能正常恢复且故障前数据不丢失，异常节点为共识节点时能参与正确的共识流程。	金融业务系统、科技产品
3	篡改节点数与故障节点数之和小于最大阈值时可正常达成全网共识	1.查阅材料 2.测试系统	1.设计文档对共识算法的最大阈值有规划和设计。 2.系统支持篡改节点数与故障节点数之和小于最大阈值能正常达成全网共识，反之不可。	金融业务系统、科技产品

6.2.6 可拓展性

可拓展性评估内容见表 14。

表14 可扩展性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	支持节点增加	1.查阅材料 2.查看系统	1.设计文档包含系统支持动态或静态增加节点的说明。	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
			2.系统支持动态或静态增加节点。	技产品
2	支持节点删除	1.查阅材料 2.查看系统	1.设计文档包含系统支持动态或静态删除节点的说明。 2.系统支持动态或静态删除节点。	金融业务系统、科技产品

6.3 智能合约

6.3.1 智能合约虚拟机

智能合约虚拟机评估内容见表15。

表15 智能合约虚拟机评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供智能合约虚拟机或容器，支持智能合约的运行	1.查阅材料 2.测试系统	1.设计文档中包含智能合约虚拟机或容器的规划说明。 2.系统智能合约虚拟机或容器经测试能支持智能合约的运行。	金融业务系统、科技产品

6.3.2 智能合约编程语言

智能合约可编程能力评估内容见表16。

表16 智能合约可编程能力评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应明确智能合约具备图灵完备性	1.查阅材料 2.查看系统	1.设计文档提供智能合约图灵完备性的说明。 2.智能合约代码实际编写与系统提供的图灵完备性说明一致。	金融业务系统、科技产品
2	应提供智能合约编程语言和配置方式	1.查阅材料 2.查看系统	1.设计文档提供对智能合约编程语言的配置说明。 2.系统按照配置说明能够开发智能合约代码。	金融业务系统、科技产品
3	应支持智能合约编程语言的主流稳定版本	1.查阅材料 2.查看系统	1.设计文档声明了智能合约编程语言是主流编程语言，主流程度符合一般公认原则，具有不局限于区块链领域的开发者开放生态。 2.系统支持的智能合约编程语言具有成熟的工具包支持，包括但不限于集成开发环境（IDE）、编译器、调试器、测试工具、持续集成工具等。	金融业务系统、科技产品

6.3.3 智能合约编译

智能合约源码编译评估内容见表17。

表17 智能合约源码编译评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应确保智能合约编译工具或方法编译结果的正确性	1.查阅材料 2.测试系统	1.设计文档提供了智能合约编译工具或方法的完整说明。 2.系统编译后的智能合约能够被正确地识别、加载和执行，输出结果与设计文档一致。	金融业务系统、科技产品
2	应提供智能合约编译工具或方法的主流稳定版本	1.查阅材料 2.查看系统	1.设计文档提供智能合约编译工具主流稳定版本的完整说明，主流程度认定符合一般公认原则。 2.系统的智能合约编译工具和方法经测试与设计文档一致。	金融业务系统、科技产品

6.3.4 智能合约正确性

智能合约正确性评估内容见表18。

表18 智能合约正确性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证执行调用智能合约能获得与参数输入相对应的正确结果	1.查阅材料 2.查看系统 3.测试系统	1.设计文档提供已部署智能合约实现的功能说明。 2.系统已部署智能合约的源代码与对应的设计文档一致。 3.系统使用正确方法调用合约操作，能够得到符合说明文档描述的正确结果；使用错误方法调用合约操作，能够得到符合说明文档描述的错误结果。	金融业务系统、科技产品

6.3.5 智能合约一致性

智能合约调用执行一致性评估内容见表19。

表19 智能合约一致性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	智能合约在各节点上的执行结果应完全相同	1.查阅材料 2.测试系统	1.设计文档提供节点同步、校验交易准确性、一致性的技术方案。 2.系统在不同节点上执行交易，得到的结果一致。	金融业务系统、科技产品
2	应在多节点同时调用同一智能合约时，各节点数据互不干扰	1.查看系统 2.测试系统	1.系统各个节点可以独自运行智能合约。 2.系统各节点同时执行同一智能合约结果相同，各节点数据互不干扰。	金融业务系统、科技产品

6.3.6 智能合约可靠性

智能合约可靠性评估内容见表20。

表20 智能合约可靠性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应实现智能合约的执行原子性	1.查阅材料 2.测试系统	1.设计文档提供智能合约原子性的详细说明。 2.系统调用智能合约执行异常操作能够正常撤回。 3.系统调用智能合约执行有效操作，各节点执行结果准确一致。	金融业务系统、科技产品
2	应支持系统运行一段时间后进行升级，升级后新的系统应可以正常运行智能合约	1.查阅材料 2.测试系统	1.设计文档提供系统升级后智能合约正常运行的详细说明。 2.系统升级后能够正确运行智能合约。	金融业务系统、科技产品

6.3.7 智能合约业务隔离性

智能合约业务隔离性评估内容见表21。

表21 智能合约业务隔离性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	不同智能合约的业务数据传输应互不干扰	1.查阅材料 2.查看系统	1.设计文档说明了从逻辑上、物理上实现不同智能合约执行环境有效隔离的方法。 2.系统隔离环境保证不相干的智能合约业务数据传输互不干扰。	金融业务系统、科技产品
2	应支持不同智能合约的业务数据存储按需隔离	1.查阅材料 2.查看系统	1.设计文档支持不同智能合约有独自的数据存储环境。 2.系统不同智能合约之间的数据未经授权不可相互访问。	金融业务系统、科技产品
3	对于没有业务依赖的不同智能合约，并行执行应互不干扰	1.查阅材料 2.查看系统	1.设计文档说明了从逻辑上、物理上实现没有业务依赖的不同智能合约有效隔离的方法。 2.系统隔离环境支持智能合约之间的数据隔离。 3.系统隔离环境支持智能合约的运行资源隔离，包括运行CPU、内存等资源隔离。	金融业务系统、科技产品
4	应对金融行业智能合约中的敏感业务逻辑进行严格授权控制	1.查阅材料 2.查看系统	1.设计文档提供完善的授权方案。 2.系统编写智能合约业务逻辑时严格按照授权方案执行。 3.系统建立有效的智能合约审核机制，只有通过审核的智能合约才能被部署，调用执行。 4.系统具备完善的成员管理机制，对于金融行业智能合约的敏感业务逻辑控制在信任度高、安全管控能力强的金融机构或监管部门，其他	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			成员仅在授权范围内使用、执行智能合约逻辑。	

6.3.8 智能合约生命周期管理

智能合约全生命周期管理评估内容见表22。

表22 智能合约全生命周期管理评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供智能合约全生命周期管理	1.查阅材料 2.查看系统	1.设计文档包含智能合约全生命周期管理的描述，如部署、运行、升级、冻结、解冻、废止等。 2.系统执行智能合约全生命周期操作能够得到正确结果。	金融业务系统、科技产品
2	应有相应机制控制智能合约的部署行为，防止恶意部署智能合约	1.查阅材料 2.查看系统	1.设计文档提供智能合约部署操作的授权说明。 2.系统由获得授权的用户在授权的节点上能够部署安装智能合约。 3.系统由未获得许可的用户或者未获得许可的节点上无法部署智能合约。	金融业务系统、科技产品
3	部署成功的智能合约应具有唯一标识	1.查阅材料 2.查看系统	1.设计文档对智能合约的唯一性标识有规划和设计，支持在不同节点查询到智能合约信息保持一致。 2.系统支持在不同节点的智能合约唯一标识信息保持一致性。	金融业务系统、科技产品
4	同一版本智能合约在不同节点上部署应保持一致	1.查阅材料 2.查看系统	1.设计文档对智能合约在不同节点上部署的一致性有规划和设计。 2.系统支持在不同节点上部署的智能合约保持一致。	金融业务系统、科技产品
5	应提供智能合约在线滚动升级方案，智能合约升级后应能正常调用智能合约	1.查阅材料 2.查看系统	1.设计文档包含智能合约在线升级的说明。 2.系统按照设计文档能够正常升级智能合约。 3.系统智能合约升级后按照最新版本调用执行，各功能正常可用。	金融业务系统、科技产品
6	应在智能合约更新升级、重新部署后，安全无误将原智能合约数据迁移至新智能合约	1.查阅材料 2.查看系统	1.设计文档中提供完整有效的数据迁移方案。 2.系统根据迁移方案可以准确无误的完成数据迁移。 3.系统提供数据校验方案，确保数据迁移过程中无异常，以及迁移数据的有效性、准确性。	金融业务系统、科技产品
7	应提供智能合约冻结功能	测试系统	系统中智能合约拥有者在满足智能合约控制策略时能对智能合约实施冻结，冻结的智能合约不能再提供服务。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
8	应提供智能合约解冻功能	测试系统	系统中智能合约拥有者在满足智能合约控制策略时能对智能合约实施解冻，解冻的智能合约可以继续提供服务。	金融业务系统、科技产品
9	应提供智能合约废止功能	测试系统	系统中智能合约拥有者在满足智能合约控制策略的前提下能废止智能合约，智能合约废止后不能解除废止状态，废止的智能合约不再提供服务。	金融业务系统、科技产品

6.3.9 智能合约版本控制

智能合约版本控制评估内容见表 23。

表23 智能合约版本控制评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应支持在部署智能合约时，指定智能合约的版本号	1.查阅材料 2.查看系统	1.设计文档提供智能合约版本号的制定规则。 2.系统部署、升级智能合约时，能按照规则指定版本号。	金融业务系统、科技产品
2	交易信息中应明确调用的智能合约版本	查看系统	1.系统调用执行智能合约时支持将版本信息记录到账本中。 2.交易完成后，系统能通过区块链浏览器在交易信息中查看到执行该交易的智能合约版本号。	金融业务系统、科技产品
3	不同节点之间的相同智能合约应保证版本一致性	1.查阅材料 2.查看系统	1.设计文档包含同一智能合约版本在不同节点之间一致的说明。 2.系统在智能合约升级完成后，具备智能合约版本号的校验检查机制，防止节点升级失败造成的节点之间智能合约版本不一致。	金融业务系统、科技产品
4	应保证智能合约升级后，交易只能调用新版本智能合约	测试系统	系统在调用智能合约时，确保调用执行最新版本号的智能合约，不能再调用老版本智能合约。	金融业务系统、科技产品

6.4 节点通信

6.4.1 组网方式

组网方式评估内容见表24。

表24 组网方式评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	节点通信的组网方式可动态配置	1.查阅材料 2.查看系统 3.测试系统	1.设计文档提供不同组网的拓扑说明、可变配置文件说明。	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
			2.系统配置文件中不同组网方式的配置参数与设计文档一致。 3.系统通过动态配置文件，节点能正常收到网络消息，组网结果与设计文档一致。	技产品
2	单一节点故障应不影响节点的整网通信	1.查阅材料 2.测试系统	1.设计文档包含单一节点故障的同步策略，包括交易同步优化策略和区块同步优化策略，保障其他节点正常通信。 2.系统在某一节点故障时，未发生故障的节点能正常通信，数据收发的同步策略与设计文档一致。	金融业务系统、科技产品
3	节点通讯应与上层业务解耦合	1.查阅材料 2.测试系统	1.开发文档或用户文档包含外部接口说明，上层业务应用可通过SDK调用接口实现节点通讯的操作，达到解耦合目的。 2.系统对外部接口的调用等操作能产生特定结果，接口功能与开发文档或用户文档一致。	金融业务系统、科技产品
4	节点通讯应实现心跳机制，保证节点的在线状态，防止因节点网络离线造成的账本不一致	1.查阅材料 2.查看系统 3.测试系统	1.设计文档提供了节点的心跳机制方案，包括但不限于维护自身的状态、定时广播等。 2.系统正常运行状态时的节点日志中存在心跳记录。 3.系统能通过心跳机制与其他节点建立连接，进行状态同步，保障账本一致性。	金融业务系统、科技产品
5	节点应能在异常场景恢复后恢复原组网功能	1.查阅材料 2.测试系统	1.设计文档中包含节点异常恢复方案，包括但不限于自身的状态检查、定时广播、与其他节点同步区块状态、自动断开异常连接、自动发起重连等。 2.系统中处于离线状态的节点恢复后，节点能够与其他节点建立连接进行状态同步，将区块状态更新到最新，恢复原组网功能。	金融业务系统、科技产品

6.4.2 消息转发

消息转发评估内容见表25。

表25 消息转发评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	消息转发的接收节点可配置	1.查看系统 2.测试系统	1.系统选择接收节点后，节点能收到预期消息。 2.系统通过修改配置文件或接口参数调整接收节点，能在预期节点上收到消息。	金融业务系统、科技产品
2	网络中的消息应有唯一的标识符	1.查阅材料 2.测试系统	1.设计文档中披露消息标识符的生成规则，保证标识符具有唯一性。	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
			2.系统通过向节点发送多条消息，各消息标识符不重复。 3.系统的消息标识符在节点转发前后一致。	技产品
3	应明确消息转发范围	1.查阅材料 2.测试系统	1.设计文档对消息转发范围有明确定义，给出能收到转发消息的节点范围。 2.系统不在消息转发范围的节点不能收到转发的消息。	金融业务系统、科技产品
4	应具备异常场景恢复机制	1.查阅材料 2.测试系统	1.设计文档对异常场景恢复机制有规划和设计，对断电、网络抖动、磁盘满、机器重启等异常场景有对应的恢复机制。 2.系统从异常场景恢复后，能够获取其他正常服务节点的状态信息并恢复消息转发功能。	金融业务系统、科技产品

6.4.3 节点加入

节点加入评估内容见表26。

表26 节点加入评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	单个节点初始化完毕后，应具备完整的通信能力	1.查阅材料 2.测试系统	1.用户文档、管理文档包含节点初始化后的完整通信和能力描述。 2.节点加入后能与区块链网络正常同步数据。	金融业务系统、科技产品
2	出现断电、重启、网络波动等异常场景恢复后，节点应具备完整的通信能力	1.查阅材料 2.测试系统	1.设计文档、开发文档包含断电、重启、网络波动等异常场景的节点恢复功能设计和开发说明。 2.用户手册包含断电、重启、网络波动等异常场景的节点恢复操作说明和操作步骤。 3.系统在异常场景恢复后，节点能正常运行。	金融业务系统、科技产品
3	应支持新节点动态在线加入网络的功能，新加入的节点不会影响原系统的正常通信	1.查阅材料 2.测试系统	1.设计文档、开发文档包含节点动态在线加入网络功能的设计和开发说明。 2.用户手册包含节点动态在线加入网络功能的操作说明和操作步骤。 3.系统具备节点动态在线加入网络功能，节点加入过程中，整个网络无异常。	金融业务系统、科技产品
4	新节点的加入应对于全网中所有已加入的节点都是等效可知的	1.查阅材料 2.测试系统	1.设计文档包含新节点申请加入网络的说明，全网中所有已加入的节点都可收到申请通知。 2.系统全网中所有已加入的节点都拥有投票权，权重一致。	金融业务系统、科技产品
5	加入新的共识或者记账节点应得到网络共识认可后才能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含对网络中加入新的共识或者记账节点多方审核说明，避免引入不可靠组织或恶意组织。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
	加入		2.系统网络中的节点独立审核新的共识或者记账节点加入请求。 3 系统具有保证审核工作开展的相关系统功能，如投票机制。	
6	加入的新节点应符合其余节点的安全验证等要求	1.查阅材料 2.测试系统	1.设计文档中包含新节点接入网络的安全要求说明。 2.新节点的加密算法与网络中的加密算法保持一致，各节点之间通信采用健壮的加密算法和安全协议保障客户端与服务器之间所有连接的安全,协议包括但不限于 TLS 和 IPSEC 等。	金融业务系统、科技产品

6.4.4 节点退出

节点退出评估内容见表27。

表27 节点退出评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应支持节点动态退出,不同节点退出对于通讯层应是无感知的,且不影响系统通信能力	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含节点动态退出实现方案，节点退出实现方案与节点通信层解耦。 2.系统配置文件中节点退出相关配置参数与设计文档一致。 3.系统测试不同类型和数量节点的动态退出，同步观测系统通信信息，结果与实现方案保持一致，节点退出操作对通讯层无感知，且不影响系统通信能力。	金融业务系统、科技产品
2	应保证节点退出并重新加入对等网络后,账本数据同步和消息通讯能够正常进行	测试系统	节点退出并重新加入对等网络后，该节点能够正确连接到其他在线节点并恢复消息通讯；数据同步完成后，该节点账本数据与其他在线节点账本数据一致。	金融业务系统、科技产品
3	应保证节点退出并重新加入共识后,节点功能正常	测试系统	节点退出并重新加入共识后，该节点能够正常运行，最终状态与其他在线节点一致。	金融业务系统、科技产品

6.5 事件分发

事件分发评估内容见表 28。

表28 事件分发评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	对于拥有不同订阅者的事件，事件分发机制应支持单点同步、多点同步或全网同步	1.查阅材料 2.查看系统 3.测试系统	1.设计方案包含对智能合约执行事件分发机制的规划和设计。 2.系统提供的接口文档与设计方案保持一致。 3.系统的同步模式测试验证结果与预期一致。	金融业务系统、科技产品
2	发布事件应包含智能合约正常执行返回结果事件和一系列的异常事件	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含对智能合约正常执行返回结果事件和一系列的异常事件功能的规划和设计。 2.系统提示的事件类型、错误码所对应的实际情况与设计文档描述相符。 3.系统经不同的（正向、反向）案例测试，能正确反馈智能合约执行信息，包括但不限于执行结果状态、执行详细信息等。	金融业务系统、科技产品
3	应通过单播、组播或广播的方式将智能合约执行结果反馈给该智能合约执行的发起者	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含向智能合约执行发起者提供单播、组播或广播方式的事件通知机制的规划和设计。 2.系统提供的接口文档与设计文档保持一致。 3.系统进行单播、组播或广播方式测试，测试结果与设计文档一致。	金融业务系统、科技产品
4	事件分发应满足时效性要求	1.查阅材料 2.测试系统	1.设计文档包含对事件时效性的规划和设计，提供保障时效的具体技术措施。 2.系统事件分发的时效性达到设计文档所声明的时效性指标。	金融业务系统、科技产品
5	应通过技术手段保证消息事件分发过程中的内容完整性和一致性	1.查阅材料 2.查看系统 3.测试系统	1.设计文档提供事件分发的安全传输机制的完整说明。 2.系统在事件分发调用过程中，只有订阅者能正确解密并获得事件信息，防止事件信息被篡改、拦截、重发。	金融业务系统、科技产品
6	应保证由于发布者系统崩溃而发布失败的事件，其包含的智能合约结果不能对本地持久化数据库有改变	测试系统	发布者系统重启恢复后，系统状态保持在交易调用之前，其智能合约结果不改变本地持久化数据库。	金融业务系统、科技产品
7	事件分发系统应有恢复机制，保证订阅者系统崩溃不影响整个系统的最终一致性	测试系统	事件分发在订阅者系统恢复后，节点能够同步获得分发事件，其分发事件的记录与其他正常节点的记录是一致的。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
8	应支持主动拉取或被动推送的事件分发能力	测试系统	1.发布者主动调用一次事件分发，订阅者能够被动接收推送的事件。 2.订阅者主动请求一次事件分发，发布者能将相应的事件发送给订阅者。	金融业务系统、科技产品

6.6 密钥管理

6.6.1 密钥生成

密钥生成评估内容见表29。

表29 密钥生成评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	用于生成密钥的随机数应满足合规性要求，且保证密钥在生成过程中的安全性	1.查阅材料 2.查看系统	1.设计文档中声明了使用的随机数生成算法经国家密码管理部门认可，并说明了密钥在生成过程中的具体安全措施。 2.系统相关安全措施的执行情况与设计文档一致。	金融业务系统、科技产品
2	密钥算法类型和密钥长度宜可配置	1.查阅材料 2.测试系统	1.设计文档中描述了密钥算法类型和长度设置的方式。 2.系统经测试能够生成不同密钥类型或长度的密钥。	金融业务系统、科技产品

6.6.2 密钥存储

密钥存储评估内容见表30。

表30 密钥存储评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	基于软件方案存储的密钥应实现对密钥的加密存储	1.查阅材料 2.查看系统	1.设计文档中描述了密钥存储类型，对于软件存储实现方式说明了密钥存储的加密算法。 2.系统使用的密钥存储加密算法与设计文档一致。	金融业务系统、科技产品
2	基于硬件方案存储的密钥应符合国家密码管理部门的硬件安全模块存储要求	1.查阅材料 2.查看系统	1.设计文档中描述了密钥存储类型，对于硬件存储实现方式说明了硬件安全模块的类型，硬件安全模块经国家密码管理部门认可。 2.系统使用的硬件安全模块符合国家密码管理部门要求。	金融业务系统、科技产品
3	应避免集中存储密钥	1.查阅材料 2.查看系统	1.设计文档中描述了如何避免集中密钥存储的方式。 2.系统使用两个或多个加密存储设备对密钥	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			进行存储，防止出现大规模密钥泄漏的风险。	
4	应使用经国家密码主管部门认可的其他类型密钥存储方式	1.查阅材料 2.查看系统	1.设计文档中描述了其他类型密钥存储的方式。 2.系统使用的其他类型密钥存储方式经国家密码管理部门认可。	金融业务系统、科技产品

6.6.3 密钥更新

密钥更新的评估内容见表31。

表31 密钥更新评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备身份验证和鉴权功能	1.查阅材料 2.测试系统 3.查看系统	1.设计文档中描述了密钥更新时需要先进行身份验证和鉴权的内容。 2.系统具备密钥更新功能且更新密钥前需要进行身份验证和鉴权。 3.系统配置信息包含身份验证与鉴权的相关信息及操作记录。	金融业务系统、科技产品
2	密钥更新后原有密钥应不能继续使用，原有密钥如果发生过交易应进行安全归档	1.查阅材料 2.测试系统	1.设计文档中明确说明了对于原有密钥使用的管理要求。 2.系统完成密钥更新后，原有密钥不能继续用来进行身份验证和鉴权。 3.系统中发生过交易的原有密钥能进行安全归档。	金融业务系统、科技产品
3	应采用密钥协商算法或机制保证密钥更新过程的安全，且更新过程中以密文形式进行密钥传输	1.查阅材料 2.访谈人员 3.测试系统	1.设计文档描述了密钥变更过程与外部交换密钥采用的机制，说明了更新过程中密钥传输方式。 2.开发人员了解密钥变更过程与外部交换密钥的机制和传输方式。 3.系统通过扫描密钥更新报文确认存在密钥协商算法及传输密文。	金融业务系统、科技产品
4	密钥更新算法应独立于业务流程	1.查阅材料 2.测试系统 3.查看系统	1.文档中明确包含了密钥更新流程设计与正常业务流程无冲突的相关要求及信息。 2.系统在新密钥进行加解密、签名验签等操作的同时，交易请求得到正确的业务结果。 3.系统日志记录了相关的密钥更新记录。	金融业务系统、科技产品

6.6.4 密钥使用

密钥使用的评估内容见表32。

表32 密钥使用评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	密钥对应按需隔离使用	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含隔离使用密钥对的功能描述。 2.系统密钥对可以通过配置隔离使用。 3.系统中隔离的密钥对交叉使用后报错。 4.系统配置中包含密钥对隔离使用配置信息。	金融业务系统、科技产品
2	应支持基于密钥对实现认证算法和签名算法	1.查阅材料 2.查看系统 3.测试系统 4.访谈人员	1.设计文档描述了可使用基于密钥对的认证算法或签名算法的内容。 2.被访谈人员确认在身份鉴别、信息完整性校验和防篡改的场景下使用认证算法和签名算法。 3.系统配置中包含使用认证算法和签名算法的信息。 4.系统的认证算法及签名算法能够正常运行。	金融业务系统、科技产品
3	应支持基于密钥对的加解密算法	1.查阅材料 2.查看系统 3.测试系统 4.访谈人员	1.设计文档中描述了可使用基于密钥对的加解密算法的内容。 2.被访谈人员确认在机密及隐私保护的场景下使用加解密算法。 3.系统配置信息中包含加解密算法相关信息。 4.系统基于密钥对的加解密算法正常运行。	金融业务系统、科技产品
4	应支持正常使用及识别密钥对	1.查看系统 2.测试系统	1.设计文档中包含密钥对的系统信息及配置项。 2.系统密钥对能正常使用，且能够识别出不同的密钥对。	金融业务系统、科技产品
5	内存应无密钥对驻留情况	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含密钥使用禁止内存驻留的规范性要求。 2.系统中无密钥驻留内存的相关信息，如日志、配置项及存储等。 3.系统经扫描内存情况确保无密钥驻留。	金融业务系统、科技产品

6.6.5 密钥撤销、销毁和归档

密钥撤销、销毁和归档评估内容见表33。

表33 密钥撤销、销毁和归档评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应支持密钥撤销和密钥销毁的功能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含密钥撤销和销毁流程描述。 2.系统配置中包含密钥撤销和销毁的相关信息。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			3.系统密钥可按流程撤销、销毁。	
2	宜支持撤销密钥归档功能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含归档功能描述及要求。 2.系统配置中包含归档动作相关记录。 3.系统对撤销后的密钥具备归档功能，归档介质满足相关安全要求。	金融业务系统、科技产品
3	撤销密钥应限制不能启用	1.查阅材料 2.测试系统	1.设计文档中包含密钥撤销后限制启用的要求。 2.系统撤销后的密钥经测试无法再次启用。	金融业务系统、科技产品

6.7 状态管理

6.7.1 查询区块高度

查询区块高度评估内容见表34。

表34 查询区块高度评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供该功能的使用说明文档	查阅材料	具备说明文档且具有查询区块高度的相关说明。	金融业务系统、科技产品
2	按照使用说明查询区块高度，应返回访问节点的最新区块高度	测试系统	按照使用说明查询区块高度，选定一个区块，系统可以查询该区块的高度，且返回高度值的最新值。	金融业务系统、科技产品
3	应能够查询出所有不同业务的区块高度	测试系统	给定一个业务类型，经查询获得该业务所有区块的区块高度。	金融业务系统、科技产品
4	应保证在节点断电、重启、网络波动等异常场景恢复后，能够继续正确支持该查询功能	测试系统	模拟节点断电、重启或网络故障恢复后，系统通过API接口完成查询功能。	金融业务系统、科技产品
5	应保证具有权限的用户能够查询到区块高度，没有权限的用户不能获取数据	1.查看系统 2.测试系统	1.具有权限的用户，系统可以通过API接口完成上述查询功能。 2.不具有权限的用户，系统无法通过API接口完成上述查询功能。 3.不具有查询权限的用户进行查询时，系统具备记录审计日志。	金融业务系统、科技产品

6.7.2 查询区块详情

查询区块详情评估内容见表35。

表35 查询区块详情评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供该功能的使用说明文档	查阅材料	功能说明文档中具备查询区块详情的接口API使用说明。	金融业务系统、科技产品
2	应能够按照说明文档使用该功能查询到区块详情，包括但不限于以下信息：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	测试系统	给定一个区块，查询获得该区块详情，包括但不限于区块高度、区块哈希值、前序区块哈希值、交易列表、区块时间戳等。	金融业务系统、科技产品
3	应能够通过区块唯一标识查询到指定区块的详情	测试系统	给定一个区块唯一标识，查询获得该区块详情，包括但不限于区块高度、区块哈希值、前序区块哈希值、交易列表、区块时间戳等。	金融业务系统、科技产品
4	应能够查询出所有不同业务的区块详情	测试系统	给定一个业务，查询得到所有包含该业务的所有区块，包括但不限于区块高度、区块哈希值、前序区块哈希值、交易列表、区块时间戳等。	金融业务系统、科技产品
5	应保证出现节点断电、重启、网络波动等异常场景恢复后，能够继续正确支持该查询功能	测试系统	节点断电、重启或网络故障恢复后，系统仍能完成查询功能。	金融业务系统、科技产品

6.7.3 查询交易信息

查询交易信息评估内容见表 36。

表36 查询交易信息评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供该功能的使用说明文档	查阅材料	功能说明文档中具备查询交易信息的接口API使用说明，入参和查询结果说明，并提供查询交易信息示例辅助说明各参数。	金融业务系统、科技产品
2	按照使用说明查询交易信息，交易信息应返回该交易详情	测试系统	通过API接口查询到交易信息，包括但不限于交易发生时间、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。	金融业务系统、科技产品
3	应能够通过交易唯一标识查询到交易	测试系统	给定一个交易唯一标识，查询出该交易的信息详情，包括但不限于交易发生时间、交易哈希	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	信息详情		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。	技产品
4	应能够查询出给定业务类型上所有交易的信息	测试系统	给定业务类型，查询获得该业务上的所有交易信息详情。	金融业务系统、科技产品
5	应保证出现节点断电、重启、网络波动等异常场景恢复后，能够继续正确支持该查询功能	测试系统	节点断电、重启或网络故障恢复后，系统仍能完成查询功能。	金融业务系统、科技产品

6.7.4 查询交易结果

查询交易结果评估内容见表 37。

表37 查询交易结果评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供该功能的使用说明文档	查阅材料	功能说明文档中具备查询交易结果的接口API使用说明。	金融业务系统、科技产品
2	应能够使用该功能查询到交易结果，包括但不限于以下信息：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	测试系统	给定一个交易，查询得到该交易的结果，包括但不限于交易唯一标识、交易发生时间、交易哈希值、交易发起者标识、交易执行结果。	金融业务系统、科技产品
3	若该交易为智能合约操作，应包括智能合约执行反馈事件的信息	测试系统	给定一个执行智能合约操作的交易，该交易包括反馈事件的信息。	金融业务系统、科技产品
4	应能够通过交易唯一标识查询到指定交易的结果	测试系统	给定一个交易唯一标识，通过API接口查询到指定的交易结果。	金融业务系统、科技产品
5	应能够查询出所有不同业务的交易结果	测试系统	通过API接口查询得到所有不同业务的交易结果。	金融业务系统、科技产品
6	节点断电、重启、网络波动等异常场景恢复后，应能够继续正确支持查询功能	测试系统	节点断电、重启、网络故障等异常场景恢复后，通过API接口正常完成查询功能。	金融业务系统、科技产品

6.7.5 查询账本状态

查询账本状态评估内容见表38。

表38 查询账本状态评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供该功能的使用说明文档	查阅材料	功能说明文档中具备查询账本状态的接口API使用说明。	金融业务系统、科技产品
2	应能够通过身份账户标识查询到指定身份账户当前状态	测试系统	给定一个身份账户标识，通过API接口查询获得该身份账户的当前状态。	金融业务系统、科技产品
3	应能够通过身份账户标示和指定查询范围，获取账户状态更新的历史记录	测试系统	给定一个身份账户标识和查询范围，通过API接口查询获得该账户状态更新的历史记录。	金融业务系统、科技产品
4	应能够通过区块唯一标识和身份账户标识查询到指定身份账户的历史状态	测试系统	给定一个区块标识和身份账户标识，通过API接口查询获得该账户的历史状态。	金融业务系统、科技产品
5	应能够通过智能合约唯一标识查询到智能合约数据最新状态	测试系统	给定一个智能合约标识，通过API接口查询获得该智能合约数据的最新状态。	金融业务系统、科技产品
6	应能够通过区块唯一标识和智能合约唯一标识查询到指定智能合约数据的历史状态	测试系统	给定一个区块标识和智能合约标识，通过API接口查询获得该智能合约数据的历史状态。	金融业务系统、科技产品
7	应保证出现节点断电、重启、网络波动等异常场景恢复后，能够继续正确支持该查询功能	测试系统	节点断电、重启或网络故障恢复后，系统通过API接口完成查询功能。	金融业务系统、科技产品

6.7.6 账本状态更新

账本状态更新评估内容见表39。

表39 账本状态更新评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供该功能的使用说明文档	查阅材料	功能说明文档中具备账本状态更新的接口API使用说明。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
2	应由交易触发账本数据状态更新	测试系统	给定一个交易，通过API接口更新账本数据状态。	金融业务系统、科技产品
3	查询到交易结果后，交易对账本状态的更新应写入账本文件	测试系统	查询到交易成功结果后，通过API接口成功查询获得该交易对账本状态的更新。	金融业务系统、科技产品
4	应保证不同节点之间账本状态更新流程的一致性，并在有限时间内达成数据状态一致性	测试系统	不同节点操作流程保持一致，给定一个有限时间区段，通过API接口查询确认账本数据状态一致。	金融业务系统、科技产品
5	应保证出现节点断电、重启、网络波动等异常场景恢复后，节点上已经更新的账本数据状态不会发生更改	测试系统	节点断电、重启或网络故障恢复后，通过API接口查询确认更新的账本数据状态没有发生更改。	金融业务系统、科技产品

6.8 成员管理

6.8.1 用户注册

用户注册评估内容见表40。

表40 用户注册评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应支持用户注册	1.查阅材料 2.查看系统	1.提供系统支持用户注册功能的相关文档。 2.查看系统用户注册，与文档保持一致。	金融业务系统、科技产品
2	应具备用户隐私保护机制	1.查阅材料 2.查看系统	1.提供完整的用户生命周期管理说明及系统实现。 2.用户信息的收集有明确的文档说明及系统实现。 3.收集用户信息能够采用明确方式获得信息主体同意。 4.信息收集、保存、传输和存储有明确的文档说明及系统实现。	金融业务系统、科技产品
3	应支持身份唯一性鉴别	1.查阅材料 2.查看系统	1.提供明确的唯一标志用户身份的说明及系统实现。 2.使用同一身份多次发起注册请求时，服务端仅成功接收一次请求，并注册成功。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			3.用户注册完成后能通过唯一身份标识发送交易。	
4	应具备用户权限设置功能	1.查阅材料 2.查看系统	1.支持普通用户、管理员等多层次权限账户。 2.管理员具有冻结和解冻其他账户的权限。	金融业务系统、科技产品
5	应具备异常场景处理功能	1.查阅材料 2.查看系统	1.节点出现断电、重启、网络波动等异常场景恢复后，节点能够继续识别用户的身份信息并接收用户发送的请求。	金融业务系统、科技产品

6.8.2 用户身份识别

用户身份识别评估内容见表41。

表41 用户身份识别评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供专门的组件或模块实现用户身份认证功能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含对用户身份认证模块说明。 2.系统源码或配置文件中体现用户主体身份信息和授权信息功能。 3.系统具备正确标识和鉴别用户主体身份信息和授权信息功能。	金融业务系统、科技产品
2	应使用安全并经国家密码管理部门认可的算法和协议	1.查阅材料 2.查看系统	1.设计文档中包含对身份认证过程中使用经国家密码管理部门认可的密码算法和协议的说明。 2.系统源码或配置文件中具备经国家密码管理部门认可的算法和协议特征。	金融业务系统、科技产品
3	应定期对用户账号的使用情况进行安全性分析	1.查阅材料 2.查看系统	1.设计文档中包含对用户账号使用情况的安全性分析方案说明。 2.系统中源码或配置文件中具备安全性分析功能，分析要素包括但不限于登录时间、登录位置、访问时长等。	金融业务系统、科技产品
4	应确保用户口令等身份认证相关凭证信息的存储安全性	1.查阅材料 2.查看系统	1.设计文档中包含对身份认证相关凭证信息的存储安全性方案说明，技术手段包括但不限于密码技术和访问控制技术等。 2.系统源码或配置文件具备保障用户身份认证相关凭证信息的存储安全性，用户身份认证相关凭证信息包括但不限于用户账号、口令等。	金融业务系统、科技产品
5	重要信息应采用双因素身份认证	1.查阅材料 2.查看系统	1.设计文档包含双因素身份认证方案说明。 2.系统源码或配置文件具备双因子身份认证规则。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
6	应保证异常场景恢复后节点正常接收请求	测试系统	1.在测试环境模拟断电、节点重启、网络故障等异常场景，异常消除后读取故障前存储的数据，全部数据均能正常读出。 2.在测试环境模拟断电、节点重启、网络故障等异常场景，异常消除后写入新数据，数据能成功写入。	金融业务系统、科技产品

6.8.3 用户权限变更

用户权限变更评估内容见表42。

表42 用户权限变更评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	用户权限变更应保证成员身份的唯一性	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含对用户权限变更的说明。 2.系统源码或配置文件具备身份唯一性特性，并且用户权限变更流程符合设计文档中的描述。 3.测试系统用户权限变更功能正常执行。	金融业务系统、科技产品
2	权限变更操作应由身份注册机构完成或发起	1.查阅材料 2.查看系统	1.设计文档中包含对权限变更操作的说明。 2.系统源码或配置文件中身份注册机构具备权限变更操作权限。	金融业务系统、科技产品
3	特殊权限授权应由身份注册机构完成授权	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含对管理员等特殊权限的授权的方案说明。 2.系统配置文件中包含的管理员等特殊权限的授权配置参数。 3.测试系统对管理员等特殊权限的授权功能正常执行。	金融业务系统、科技产品
4	用户权限信息变更后应在不同节点间同步	测试系统	测试系统用户权限信息变更功能正常执行，并且访问其他节点可以看到权限变更结果在多节点同步。	金融业务系统、科技产品
5	用户权限变更后应能够正常使用新权限所赋予的操作	测试系统	测试系统用户权限信息变更功后新授权功能正常使用。	金融业务系统、科技产品
6	用户权限变更后应不能再使用旧权限所赋予的操作	测试系统	测试系统用户权限信息变更功后旧授权功能无法正常使用。	金融业务系统、科技产品
7	应保证异常场景恢复后节点正常接收请求	测试系统	1.在测试环境模拟断电、节点重启、网络故障等异常场景，异常消除后读取故障前存储的数据，全部数据均能正常读出。 2.在测试环境模拟断电、节点重启、网络故障等异常场景，异常恢复后能成功写入新数据。	金融业务系统、科技产品

6.8.4 用户角色授权

用户角色授权评估内容见表43。

表43 用户角色授权评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应设立治理者角色	1.查阅材料 2.查看系统	1.提供治理者角色功能的相关文档。 2.查看系统用户列表，存在治理者角色。	金融业务系统、科技产品
2	治理者角色应具备用户管理权限	测试系统	1.治理者角色能够对目标用户进行注销、冻结等操作。 2.完成共识后，目标用户状态按照预期变化。	金融业务系统、科技产品
3	应支持多种用户角色授权	1.查阅材料 2.查看系统	1.具备支持多种用户角色授权功能的文档。 2.查看系统用户列表，与文档保持一致。	金融业务系统、科技产品
4	用户角色权限的回收应经过共识	测试系统	系统中包括治理者角色在内，所有角色权限的授权和回收都经过共识。	金融业务系统、科技产品

6.8.5 用户账户冻结和解冻

用户账户冻结和解冻评估内容见表44。

表44 用户账户冻结和解冻评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应支持账户冻结	测试系统	1.注册机构发起冻结请求，目标用户状态改为冻结。 2.完成共识后，用户状态变为冻结。	金融业务系统、科技产品
2	冻结状态应同步到所有节点	测试系统	在其他节点查询用户状态，结果为冻结状态。	金融业务系统、科技产品
3	冻结状态的用户应不能发起交易	测试系统	冻结用户发起交易请求，请求被拒绝。	金融业务系统、科技产品
4	应保证节点异常场景恢复后，节点能继续识别用户的冻结状态	测试系统	1.节点出现断电或重启，重新上电，完成与其他正常节点同步。 2.查询用户状态，结果与其他正常节点的数据一致。	金融业务系统、科技产品
5	应支持账户解冻	测试系统	1.注册机构发起解冻请求，目标用户状态改为解冻。 2.完成共识后，用户状态变为解冻。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
6	解冻状态应同步到所有节点	测试系统	在其他节点查询用户状态，结果为解冻状态。	金融业务系统、科技产品
7	解冻用户应能正常发起交易	测试系统	1.冻结用户解冻后，能够发起交易请求。 2.共识完成后，可以查询到交易记录。	金融业务系统、科技产品
8	应保证节点异常场景恢复后，能继续识别用户解冻状态	测试系统	1.节点出现断电或重启，重新上电，完成与其他正常节点同步。 2.查询用户状态，结果与其他正常节点的数据一致。	金融业务系统、科技产品

6.8.6 用户注销

用户注销评估内容见表45。

表45 用户注销评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	账户应设定使用期限	1.查看系统 2.测试系统	1.系统的账户字段包含使用期限或类似字段。 2.测试模拟注册一个已到期或将到使用期限的账户，等待到使用期限到期，检查该账户已被注销。	金融业务系统、科技产品
2	应提供注销申请功能	1.查阅材料 2.测试系统	1.文档材料中具备账户注销申请的相应说明。 2.按账户注销功能说明，测试提交注销申请功能后，目标账户状态能及时变更为注销。	金融业务系统、科技产品
3	应能重置公私钥对	1.查阅材料 2.测试系统	1.文档材料中具备账户公私钥重置方法的说明。 2.测试系统，根据材料说明的公私钥重置方法重置指定账户公私钥对，公私钥对重置成功，并且指定账户的用户身份标识没有改变。	金融业务系统、科技产品
4	应保留已注销用户登记信息和身份标识	测试系统	1.注销指定账户后，系统中能够查询到对应的信息。 2.注销指定账户后，尝试注册新的账户，新账户的身份标识与注销的账户不一致。 3.若自定义账户身份标识，使用注销账户的身份标识尝试注册新的账户，注册申请被拒绝。	金融业务系统、科技产品
5	用户信息在注销后应能够同步通知到所有节点	测试系统	1.通过节点发起用户注销申请并成功后，在其他通讯正常的节点查看该用户信息，用户状态为已注销。 2.通过节点发起用户注销申请并成功后，在其他通讯正常的节点使用该用户进行的交易被拒绝。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
6	注销用户应无法进行交易	测试系统	注销用户后，使用该用户发起交易，该交易被拒绝。	金融业务系统、科技产品
7	节点应能在异常恢复后识别用户的身份已经注销并拒接用户发送的请求	测试系统	1.对指定节点所在物理设备进行断电、重启、断网等操作，使用已注销用户向该节点发起交易，交易被拒绝。 2.关闭指定节点进程，在其他节点发起用户注销申请并确认成功注销，重启指定节点后，使用该注销用户向该节点发起交易，交易被拒绝。	金融业务系统、科技产品

6.8.7 用户信息查询

用户信息查询评估内容见表46。

表46 用户信息查询评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应通过用户唯一标识查询成员身份信息	1.查阅材料 2.测试系统	1.设计文档对查询成员身份信息有规划和设计，支持通过用户唯一标识查询成员身份信息。 2.设计文档为开发人员提供查询成员身份信息接口API。 3.系统支持通过用户身份唯一标识查询成员身份信息。	金融业务系统、科技产品
2	注册机构应有权查询用户所有信息	1.查阅材料 2.测试系统	1.设计文档对查询所有用户身份信息有规划和设计，支持注册机构查询用户所有信息，其他用户只有查询个人身份信息的权限。 2.设计文档为开发人员提供注册机构查询所有用户信息接口API。 3.系统支持注册机构查询用户所有信息。	金融业务系统、科技产品
3	不同节点查询的用户信息应保持一致	1.查阅材料 2.测试系统	1.设计文档对不同节点查询用户信息一致性有规划和设计，支持在不同节点查询用户信息保持一致。 2.系统支持在不同节点查询的用户信息保持一致性。	金融业务系统、科技产品
4	应支持用户查询身份冻结信息	1.查阅材料 2.测试系统	1.设计文档对查询用户冻结状态有规划和设计，支持在用户处于冻结状态下查询身份信息处于冻结。 2.系统支持在用户处于冻结状态下能够查询身份信息处于冻结。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
5	用户解冻后应能查询到用户当前的账户信息	1.查阅材料 2.测试系统	1.设计文档对解除冻结用户查询用户信息有规划和设计，支持在用户解除冻结后查询用户当前的账户信息。 2.系统支持用户解除冻结后查询用户当前的账户信息。	金融业务系统、科技产品
6	应能查询到用户身份的权限信息	1.查阅材料 2.测试系统	1.设计文档对查询用户权限信息有规划和设计，支持用户查询用户身份的权限信息。 2.设计文档为开发人员提供查询用户身份权限信息接口API。 3.系统支持用户查询用户身份的权限信息。	金融业务系统、科技产品
7	应能查询到用户当前的账户信息	1.查阅材料 2.测试系统	1.设计文档对查询用户账户信息有规划和设计，支持用户查询用户当前的账户信息。 2.设计文档为开发人员提供查询用户当前账户信息接口API。 3.系统支持用户查询用户当前的账户信息。	金融业务系统、科技产品
8	应保证异常场景恢复后从节点查询到的用户信息保持一致	1.查阅材料 2.测试系统	1.设计文档对异常场景恢复后查询用户信息一致性有规划和设计，支持在节点出现断电、重启、网络波动等异常场景恢复后查询的用户信息保持一致。 2.系统支持在节点出现断电、重启、网络波动等异常场景恢复后查询的用户信息保持一致。	金融业务系统、科技产品

6.8.8 用户交易

用户交易评估内容见表47。

表47 用户交易评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应能通过用户身份唯一标识发起业务交易，并达到预期的交易结果	1.查阅材料 2.查看系统 3.测试系统	1.说明文档提供用户交易步骤。 2.用户登录对应的，系统提供查询其唯一的标识。 3.用户发起交易，应能达到预期的交易结果。	金融业务系统、科技产品
2	应支持同一笔交易完成一账户向另一个账户的交易	测试系统	用户登录账户向其他账户发起交易，能够获得交易收据，并根据交易收据核验交易成功。	金融业务系统、科技产品
3	应支持同一消息请求完成一个账户向多个账户的转账交易	测试系统	用户登录账户，发送一个交易请求消息，包含该账户向多个其他账户转账的交易请求，交易完成后获得交易收据，可根据交易收据核验交易成功。	金融业务系统、科技产品
4	应保证节点异常场景恢复后，查询到的	测试系统	节点出现断电或重启，重新上电，完成与其他正常节点同步。系统查询用户账户数据修	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	用户账户数据修改与交易修改保持一致		改和交易修改，查询结果与其他正常节点的数据一致。	技产品
5	应该支持自组生态内自由订阅上架智能合约信息	1.查阅材料 2.查看系统	1.提供上架智能合约信息说明文档。 2.提供上架智能合约信息功能，便于相关用户订阅。	金融业务系统、科技产品

6.9 交易系统

6.9.1 智能合约部署交易

若支持智能合约部署，智能合约部署交易评估内容见表48。

表48 智能合约部署交易评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供智能合约部署交易功能的说明	查阅材料	1.设计文档中包含智能合约部署交易的功能说明。 2.安装手册中包含智能合约部署交易的操作说明。	金融业务系统、科技产品
2	应可获取智能合约部署交易的唯一标识	查看系统	在智能合约部署完成后，系统具备在数据库及日志中存储该智能合约部署交易的唯一标识的功能。	金融业务系统、科技产品
3	应对交易的内容进行验证，验证内容包括但不限于：数据格式有效性、签名有效性、权限、智能合约执行要求，参数合法性	1.查阅材料 2.测试系统	1.设计文档中包含智能合约部署交易的功能说明，包括但不限于数据格式有效性、签名有效性、权限、智能合约执行要求、参数合法性等内容。 2.测试案例及记录单包含该智能合约部署交易对应的验证记录，且与设计文档中功能说明一致，验证内容包括但不限于验证数据格式有效性、签名有效性、权限、智能合约执行要求、参数合法性等内容。 3.在智能合约部署完成后，系统具备该智能合约的测试交易，数据格式有效性、签名有效性、权限、智能合约执行要求、参数合法性等内容与设计文档中功能说明一致。	金融业务系统、科技产品
4	可通过交易唯一标识获取部署成功的智能合约唯一标识，部署结果应与预期一致	查看系统	1.系统中包含相应的查询交易，通过智能合约部署完成后返回的交易唯一标识查询相应的智能合约部署交易详细信息，并返回交易唯一标识。 2.系统日志显示该智能合约部署交易已成功，且日志中应显示该交易的关键信息，如发起	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			人、时间戳、哈希值等。	
5	应提供部署时定义版本号功能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中明确部署合约的版本号设定方法以及规则。 2.系统API中可以通过设定版本号部署合约，其设定方法和规则与设计文档一致。 3.系统具备支持智能合约部署时定义版本号的功能。	金融业务系统、科技产品
6	应保证出现节点断电、重启、网络波动等异常场景下，部署结果应与预期一致	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含对节点断电、重启、网络波动等异常场景的对策设计。 2.设计文档包含具体的异常应对策略。 3.系统配置中包含针对异常应对的说明，与设计文档中配置目标一致。 4.系统中测试一定比例节点发生异常时，调用智能合约部署交易的结果与预期一致。	金融业务系统、科技产品
7	应控制智能合约的部署操作，防止恶意部署行为，没有权限的节点部署调用智能合约应失败	1.查阅材料 2.测试系统	1.设计文档中对部署有权限控制,对于智能合约部署行为有对应手段进行审核或限制。 2.设计文档中对权限控制和方案一致。 3.非授权的节点部署调用智能合约失败。	金融业务系统、科技产品
8	应提供智能合约在线升级部署方案，智能合约升级部署后应能正常调用智能合约	1.查阅材料 2.测试系统	1.设计文档中对智能合约在线升级功能有支持。 2.设计文档中对智能合约在线升级功能的方式和设计文档一致。 3.系统支持智能合约在线升级，升级后原智能合约数据使用不受影响，若有影响，有相关的使用说明。	金融业务系统、科技产品
9	应在智能合约更新升级、重新部署后，能安全无误将原智能合约数据迁移至新智能合约	1.查阅材料 2.查看系统	1.数据迁移方案包含相应说明：智能合约数据迁移时是否需要系统停止对外提供服务，不同类型的节点数据迁移方案是否有差别，迁移完成后如何处理旧合约数据。 2.智能合约升级完成后，旧版本的智能合约数据在系统中保留或存有备份。	金融业务系统、科技产品

6.9.2 智能合约方法调用交易

智能合约调用方法评估内容见表49。

表49 智能合约调用方法评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供通过交易调用智能合约方法的功能	1.查阅材料 2.测试系统	1.设计文档中包含通过交易调用智能合约方法的说明和对交易的定义。 2.设计文档包含为开发人员提供通过交易调用智能合约的API，并与设计文档中对该部分的描述保持一致。 3.系统具备通过交易调用智能合约的能力，并且能正确返回预期结果。	金融业务系统、科技产品
2	应提供通过智能合约调用交易功能的说明	查阅材料	在设计文档中包含对该功能的描述说明。	金融业务系统、科技产品
3	应能够通过智能合约标识及其方法标识来调用智能合约中的方法	1.查阅材料 2.测试系统	1.设计文档中包含通过智能合约标识及其方法标识调用智能合约的描述。 2.系统具备通过智能合约标识及其方法标识调用智能合约方法的能力。	金融业务系统、科技产品
4	应能够对交易的内容进行验证	1.查阅材料 2.测试系统	1.设计文档中包含对交易验证的具体内容的描述。 2.系统中测试交易验证参数，与设计文档中的描述一致。	金融业务系统、科技产品
5	应能够获取调用智能合约交易的唯一标识	1.查阅材料 2.测试系统	1.设计文档中包含获取智能合约交易唯一标识的描述。 2.系统通过交易调用智能合约，具备返回该交易唯一标识的能力。	金融业务系统、科技产品
6	应能够通过交易唯一标识获取智能合约执行的正确结果	1.查阅材料 2.测试系统	1.设计文档中包含通过交易的唯一标识获取智能合约执行结果这一功能的描述。 2.通过系统的查询接口测试，具备通过交易标识获取智能合约执行正确结果的能力。	金融业务系统、科技产品
7	应保证出现节点异常的情况下，调用交易的结果与预期一致	1.查阅材料 2.测试系统	1.设计文档中应包含对异常容错的具体描述。 2.系统中实际测试一定比例节点发生异常的情况下，调用交易的结果与预期一致。	金融业务系统、科技产品
8	应提供通过交易调用智能合约的访问控制机制	1.查阅材料 2.测试系统	1.设计文档中包含智能合约调用的访问控制机制的具体描述。 2.系统进行智能合约调用测试，具备智能合约访问控制的能力。	金融业务系统、科技产品

6.9.3 原生交易

若提供原生交易功能，原生交易评估内容见表50。

表50 原生交易评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供支持的原生交易功能列表和功能列表的说明列表	1.查阅材料 2.查看系统	1.提供本系统支持原生交易功能列表的完整说明。 2.系统具备原生交易功能列表，保证其与说明文档一致。	金融业务系统、科技产品
2	应支持发送原生交易，可获取交易唯一标识，对交易的内容进行验证，验证内容包括但不限于：数据格式有效性、签名有效性、权限，参数合法性；应能根据交易唯一标识获取交易结果，并和预期一致	测试系统	1.发起一次原生交易，可生成唯一的原生交易标识。 2.系统根据交易标识，对交易的内容进行验证，验证内容包括但不限于：数据格式有效性、签名有效性、权限，参数合法性。 3.系统可以根据唯一的交易标识，查询得到交易结果，核实交易正常执行。	金融业务系统、科技产品
3	应保证出现节点断电、重启、网络波动等异常场景下，节点恢复后可获取交易的结果的一致性	测试系统	节点出现断电或重启，重新上电，完成与其他正常节点的数据同步，系统可以根据唯一的交易标识，查询得到交易结果，查询结果与其他正常节点一致。	金融业务系统、科技产品

6.9.4 交易原子性

交易原子性评估内容见表51。

表51 交易原子性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证交易中包含的所有数据状态更新的原子性	1.查阅材料 2.查看系统	1.设计文档中包含对数据状态更新时保证交易原子性的方案进行说明。 2.设计文档中对数据状态更新的原子性机制和设计文档一致。 3.系统中源码或配置文件中所体现的数据状态更新的原子性符合设计文档中的描述。	金融业务系统、科技产品
2	应保证交易失败回退的情况下,交易中包含的所有数据状态回退的原子性	1.查阅材料 2.查看系统	1.设计文档中包含对交易失败回退时保证交易原子性的方案进行说明。 2.设计文档中对数据状态回退的原子性机制和设计文档一致。 3.系统中源码或配置文件中所体现的数据状	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			态回退的原子性符合设计文档中的描述。	
3	应保证出现节点断电、重启、网络波动等异常场景下,交易执行、回退的原子性	1.查阅材料 2.查看系统	1.设计文档中包含对节点断电、重启、网络波动等异常场景下保证交易原子性的方案进行说明。 2.设计文档中对节点断电、重启、网络波动等异常场景下保证交易原子性的机制和设计文档一致。 3.系统中源码或配置文件中所体现的在节点断电、重启、网络波动等异常场景下保证交易原子性的机制符合设计文档中的描述。	金融业务系统、科技产品

6.10 接口管理

6.10.1 外部接口

外部接口评估内容见表52。

表52 外部接口评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	传入分布式系统的数据应是可信的外部数据源,外部接口宜做限定来确保数据源的真实可信	1.查阅材料 2.测试系统	1.系统接口文档中提供了外部数据源接入用户的账户安全认证方案，对使用的密码产品、时间源、时间戳技术等有安全可靠性要求。 2.外部接口接入采取电子签名、电子数据摘要等技术手段确保数据不可篡改；或者数据修改后能否被发现。	金融业务系统、科技产品
2	外部接口应设置白名单制度	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含外部接口访问白名单及权限控制的说明，仅拥有管理员权限用户可设置访问白名单。 2.外部接口访问调用时采取数字证书方式保证其身份真实性。经鉴权成功后，调用预言机服务。 3.数据传输设备满足电子数据传输要求的安全功能，已正确启用和配置相关功能，并且日常运维流程中有保障此范围内功能的条款。	金融业务系统、科技产品
3	系统应明确告知用户外部方法调用	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含接口调用方法的说明。 2.系统提供了调用接口示例。 3.系统提供了接口调用测试沙箱环境。	金融业务系统、科技产品
4	应保证数据源传输到分布式系统的过程中,数据真实可靠	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含外部数据源传输数据到系统的安全通讯设计，对实现方式有完整说明，能够保证数据的真实可靠不被篡改。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
	不被篡改，且传输到分布式系统中后，应保证各节点上数据的一致性		2.设计文档中包含系统存储外部数据结果基于节点共识描述。 3.系统配置文件中外部接口安全通信配置参数、节点的配置以及安全配置与设计文档一致。 4.安全工具扫描探测，测试外部接口传输数据到系统的流程，接口传入的数据无法进行篡改、替换，如果被更改会返回失败提示。 5.系统收到接口测试数据后，每个节点上的数据测试结果符合预期结果。	
5	应支持可信执行环境，保证数据处理过程的可信安全	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含外部数据可信执行环境完整设计，支持至少两种的可信环境执行方案。 2.设计文档为开发人员提供不同类型的可信执行环境的接口API，并与设计文档支持的可信执行环境类型和版本一致。 3.系统配置文件包含可信执行环境参数配置，符合设计文档。 4.系统中网络和主机访问控制策略支持所用类型可信执行环境。 5.安全工具扫描探测和攻击测试，测试可信环境数据执行，测试结果符合预期结果。	金融业务系统、科技产品

6.10.2 用户接口

用户接口评估内容见表53。

表53 用户接口评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供用户接口的详细说明文档	查阅材料	1.接口说明中有接口功能和接口使用方式的详细说明。 2.接口说明中包含接口功能的详细描述，包括接口的通信协议标准、格式要求、输入输出参数、返回值等信息。其中对于接口的参数至少包括参数的类型、参数取值范围等信息。 3.接口文档中有接口的错误码含义及产生原因相关描述。 4.接口手册为开发人员提供与设计实现版本一致的说明。	金融业务系统、科技产品
2	应对接口设置访问权限	1.查阅材料 2.查看系统	1.设计文档对接口的访问控制有规划和设计，支持用户的权限管理到接口的粒度。用户对接口的访问有鉴权机制。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			2. 设计文档为开发人员提供针对不同用户对不同接口的鉴权机制及访问权限要求的详细描述。 3. 系统配置文件中用户的鉴权机制配置和接口访问控制配置与设计文档一致。	
3	应至少支持一种语言的 SDK 或者中间件	1. 查阅材料 2. 查看系统 3. 测试系统	1. 设计文档对支持的不同语言的SDK或中间件有规划和设计。 2. 设计文档对不同开发语言的SDK或中间件支持的功能和接口保持一致。 3. 设计文档为开发人员提供不同开发语言的SDK或中间的说明，并与设计实现支持的SDK或中间件保持一致。 4. 系统配置文件中不同开发语言的SDK和中间件的配置参数与设计文档一致。	金融业务系统、科技产品
4	针对不同版本的区块链系统，应提供对应版本的所有相关接口文档	1. 查阅材料 2. 查看系统	1. 设计文档对不同版本区块链系统，提供对不同接口层、不同版本的接口规划和设计。 2. 接口文档内对于不同版本系统涉及的接口有详细的功能描述及差异性解释。	金融业务系统、科技产品

6.10.3 管理接口

管理接口评估内容见表54。

表54 管理接口评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供管理接口说明	1. 查阅材料 2. 查看系统 3. 测试系统	1. 设计文档包含明确的管理接口功能说明。 2. 设计文档包含为开发人员提供对管理接口的功能、格式、方法、参数、返回值、使用方式等进行详细说明，接口文档包含完整的错误码和含义。 3. 系统管理接口的实现与设计文档说明一致。 4. 设计文档提供接口说明，支持编写测试脚本进行管理接口测试。 5. 系统能够监控管理接口健康状态。 6. 系统能够记录管理接口操作日志，并提供日志格式及详细说明。	金融业务系统、科技产品
2	应保证只有登录节点服务器的管理员，才能访问系统管理员级别的运维接口	1. 查阅材料 2. 查看系统 3. 测试系统	1. 设计文档包含管理接口访问方式及权限控制说明。 2. 系统在接受管理员访问运维接口时，具有判断管理员是否已登录节点服务器的判断，且与方案说明一致。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			3.系统中只有登录节点服务器的管理员才能访问系统管理员级别的运维接口。 4.设计文档包含管理员的职责和权限。 5.设计文档具备符合系统管理员登录、注销和注册机制的安全规范和标准。	
3	应确保系统管理员能使用管理接口创建不同级别的用户，并设置用户可访问的接口	1.查阅材料 2.测试系统	1.设计文档包含管理接口创建用户的说明。 2.设计文档包含支持 RBAC 等角色权限控制方案和说明。 3.文档包含明确的系统管理员的职责和权限，并与实际相符。 4.系统能完成用户创建，创建后的用户及其权限分配与设计文档相关说明一致。 6.系统具备记录用户访问日志，便于监管审计。	金融业务系统、科技产品
4	应控制系统管理员数目,并保证其安全性	1.查阅材料 2.测试系统	1.设计文档包含系统管理员用户数量限制的说明及系统管理员账户安全性设计的说明。 2.设计文档含有系统管理员登录、注销和注册机制的安全规范和标准。 3.系统管理用户创建数量与设计说明的一致。 4.系统管理账户的安全性与设计文档相关要求一致。	金融业务系统、科技产品
5	应确保管理接口仅做管理使用,并与其他接口分离	1.查阅材料 2.查看系统 3.测试系统	1.设计文档含有管理接口和其他接口有效隔离的设计说明。 2.系统配置可以看到管理接口和其他接口的有效隔离措施，且与方案说明一致。 3.系统中无法通过管理接口访问其他功能，通过其他接口也无法访问管理功能。	金融业务系统、科技产品

6.10.4 系统间接口

系统间接口评估内容见表55。

表55 系统间接口评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应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	1.查阅材料 2.查看系统	1.提供系统间接口说明，指明对应的系统版本。 2.系统间对应版本系统的实际调用表现与接口说明一致。	金融业务系统、科技产品
2	应具有鉴权机制用于控制对接口的访	1.查阅材料 2.查看系统	1.提供系统间接口鉴权机制的完整说明。 2.系统间接口的鉴权机制说明与系统的实际	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	问权限	3.测试系统	调用表现一致。 3.系统间接口的鉴权机制包括身份鉴别、角色授权等能力。 4.系统间接口鉴权机制的身份鉴别能区分合法系统用户和不合法系统用户。 5.系统间接口的鉴权机制的角色授权能对不同角色的合法系统用户分配不同范围的可访问接口清单。 6.每一个接口得到授权后才能访问，包括进行授权操作的接口本身。 7.每一次授权和鉴权都经过系统的所有共识节点达成共识。	技产品
3	应能通过系统间接口访问其他区块链系统	1.查阅材料 2.测试系统	1.提供本系统支持访问的其他系统类型和版本的完整说明，包括数据格式说明。 2.对支持的其他系统的数据访问与文档说明一致。	金融业务系统、科技产品
4	应提供系统间接口使其他区块链系统能访问本系统	1.查阅材料 2.测试系统	1.设计文档、开发文档包含本系统提供访问的其他系统类型和版本的完整说明，包括接口版本、数据格式等内容。 2.其他系统通过本系统提供的系统间接口进行数据访问时的表现与文档说明一致。	金融业务系统、科技产品

7 性能评估

7.1 交易吞吐率

交易吞吐率评估内容见表56。

表56 交易吞吐率评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	原生交易吞吐率应不低于最小软硬件条件下所申明的数值	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含系统基本组网拓扑结构及其节点最小软硬件配置条件下的原生交易吞吐率数值的申明。 2.系统能够满足原生交易吞吐率最小软硬件条件。 3.在基本组网拓扑结构及节点最小软硬件条件的测试环境下，系统所测试到的实际原生交易吞吐率不低于所申明的数值。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
2	最大原生交易吞吐率需要的软硬件条件下，实际原生交易吞吐率应不低于所申明的数值	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含系统最大原生交易吞吐率指标及所需的系统结构和软硬件条件。 2.系统能够满足最大原生交易吞吐率时所需的软硬件条件。 3.在最大原生交易吞吐率需要的软硬件条件的测试环境下，系统所测试到的实际原生交易吞吐率不低于所申明的数值。	金融业务系统、科技产品
3	应在异常场景发生并恢复后仍能维持原生交易性能	测试系统	1.系统在断电、重启、网络波动等异常场景恢复后的最大原生交易吞吐率数值与故障发生前基本一致。 2.异常场景恢复后保证系统各节点设备的内存、CPU、网络带宽等资源占用率均能在设计时间内恢复正常。	金融业务系统、科技产品
4	智能合约调用吞吐率应不低于最小软硬件条件下所申明的数值	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含系统最小软硬件条件下的智能合约调用吞吐率数值的申明。 2.系统能够满足智能合约调用吞吐率最小软硬件条件。 3.在最小软硬件条件的测试环境下，所测试到的实际智能合约调用吞吐率不低于所申明的数值。	金融业务系统、科技产品
5	最大智能合约调用吞吐率所需要的软硬件条件下，智能合约调用吞吐率应不低于所申明的数值	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中包含系统最大智能合约调用吞吐率指标及所需的软硬件条件。 2.系统能够满足最大智能合约调用吞吐率时所需的软硬件条件。 3.在最大智能合约调用吞吐率需要的软硬件条件的测试环境下，系统所测试到的实际智能合约调用吞吐率不低于所申明的数值。	金融业务系统、科技产品
6	应在异常场景发生并恢复后仍能维持智能合约调用交易性能	测试系统	1.系统在断电、重启、网络波动等异常场景恢复后的最大智能合约调用吞吐率数值与故障发生前基本一致。 2.异常场景恢复后系统内存、CPU、网络带宽等资源占用率恢复正常。	金融业务系统、科技产品

7.2 查询吞吐率

查询吞吐率评估内容见表57。

表57 查询吞吐率评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	块信息查询吞吐率应不低于申明的数值	1.查阅材料 2.测试系统	1.设计文档中包含特定软硬件环境下的块信息查询吞吐率数值。	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
			2.在文档材料中要求的环境下，系统并发查询块信息，统计块信息查询吞吐率不低于申明数值。	技产品
2	节点应能在异常场景恢复后保持块信息查询吞吐率	测试系统	节点在断电、重启、网络波动等异常场景恢复后，系统块信息查询信息吞吐率与故障发生前基本一致。	金融业务系统、科技产品
3	交易信息查询吞吐率应不低于申明数值	1.查阅材料 2.测试系统	1.设计文档中包含特定环境下的交易信息查询吞吐率数值。 2.在文档材料中要求的环境下，系统并发查询交易信息，统计交易信息查询吞吐率不低于申明数值。	金融业务系统、科技产品
4	节点应能在异常场景恢复后继续保证交易信息查询吞吐率	测试系统	节点在断电、重启、网络波动等异常场景恢复后，系统交易信息查询吞吐率与故障发生前基本一致。	金融业务系统、科技产品
5	交易结果查询吞吐率应不低于申明数值	1.查阅材料 2.测试系统	1.设计文档中包含特定环境下的交易结果查询吞吐率数值。 2.在文档材料中要求的环境下，系统并发查询交易结果，查询吞吐率不低于申明数值。	金融业务系统、科技产品
6	节点应能在异常场景恢复后继续保证交易结果查询吞吐率	测试系统	节点在断电、重启、网络波动等异常场景恢复正常后，交易结果查询吞吐率与故障发生前基本一致。	金融业务系统、科技产品
7	智能合约数据查询吞吐率宜不低于申明数值	1.查阅材料 2.测试系统	1.系统文档中包含特定环境下的智能合约数据查询吞吐率数值。 2.在文档材料中要求的环境下，系统并发查询智能合约相关账本数据，智能合约数据查询吞吐率不低于申明数值。	金融业务系统、科技产品
8	节点宜在异常场景恢复后继续保证智能合约数据查询吞吐率	测试系统	节点在断电、重启、网络波动等异常场景恢复正常后，智能合约数据查询吞吐率与故障发生前基本一致。	金融业务系统、科技产品
9	历史数据查询吞吐率宜不低于申明数值	1.查阅材料 2.测试系统	1.设计文档中包含特定环境下的历史数据查询吞吐率数值。 2.在文档材料中要求的环境下，系统并发查询历史数据，查询吞吐率不低于申明数值。	金融业务系统、科技产品
10	节点宜在异常场景恢复后继续保证历史数据查询吞吐率	测试系统	节点在断电、重启、网络波动等异常场景恢复正常后，历史数据查询吞吐率与故障发生前基本一致。	金融业务系统、科技产品

7.3 交易同步性能

交易同步性能评估内容见表58。

表58 交易同步性能评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	最大交易广播速率应不低于申明的数值	1.查阅材料 2.测试系统	1.设计文档申明了最大交易广播速率。 2.节点持续广播交易提供账本数据同步，在不造成网络拥塞的情况下，发送交易的最大速率不低于设计文档中申明的数值。	金融业务系统、科技产品
2	交易的冗余率应不高于申明的数值	1.查阅材料 2.测试系统	1.设计文档申明了交易的冗余率。 2.节点持续发送不同的交易同步请求，节点收到的冗余交易比例不高于文档中申明的数值。	金融业务系统、科技产品
3	交易广播时延应不高于申明的数值	1.查阅材料 2.测试系统	1.设计文档申明了交易广播时延。 2.节点广播交易提供账本数据同步，测试该交易分别同步到全网25%、50%、75%、100%节点时所消耗的时间不高于文档中申明的数值。	金融业务系统、科技产品
4	节点应能在异常场景恢复后继续保证申明的交易同步性能及时延	1.查阅材料 2.测试系统	1.设计文档申明了交易同步性能及时延数值。 2.节点在断电、重启、网络波动等异常场景恢复后，提供广播及同步交易的速率、同步外部账本数据的时延均能够满足设计文档要求。	金融业务系统、科技产品
5	若支持无交易出空块，同步空块的速率应不低于申明值	1.查阅材料 2.测试系统	1.设计文档申明了同步空块的速率。 2.在无负载的情况下，节点从其他节点同步或向其他节点同步空块的速率不低于文档中申明的数值。	金融业务系统、科技产品
6	若支持无交易出空块，空块广播时延应不高于申明值	1.查阅材料 2.测试系统	1.设计文档申明了空块广播时延。 2.节点向全网广播一个空块，该区块分别同步到全网25%、50%、75%、100%节点时所消耗的时间不高于文档中申明的数值。	金融业务系统、科技产品
7	若支持无交易出空块，节点应能在异常场景恢复后继续保证申明的空块同步性能及时延	1.查阅材料 2.测试系统	1.设计文档申明了空块同步性能及时延数值。 2.在无负载的情况下，目标节点在断电、重启、网络波动等异常场景恢复正常后，能够广播及同步块，同步块的速率及广播块的时延均能够满足设计文档要求。	金融业务系统、科技产品
8	同步满负载区块的速率应不低于申明值	1.查阅材料 2.测试系统	1.设计文档申明了同步满负载区块的速率。 2.节点从其他节点同步完整账本数据的速率不低于文档中申明的数值。	金融业务系统、科技产品
9	满负载区块广播时延应不高于申明值	1.查阅材料 2.测试系统	1.设计文档申明了满负载区块广播时延。 2.节点广播完整账本数据，账本数据推送到指定节点完成账本同步所消耗的时间不高于文档中申明的数值。	金融业务系统、科技产品
10	节点应能在异常场景恢复后继续保证申明	1.查阅材料 2.测试系统	1.设计文档申明了满负载块同步性能及时延数值。	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	的满负载块同步性能及时延		2.目标节点在断电、重启、网络波动等异常场景恢复后，能够广播及同步完整账本数据，数据同步速率及完成账本数据同步的时延均满足设计文档要求。	技产品

7.4 部署效率

部署效率评估内容见表 59。

表59 部署效率评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	宜在60min内完成系统搭建	测试系统	自准备系统搭建所需安装软件、配置文件，到依次启动各节点的安装程序并测试系统出块、交易处理、查询等功能正常所消耗的时间小于60min。	金融业务系统、科技产品
2	宜在10min内完成系统的节点扩容	测试系统	对共识或记账节点执行内存、磁盘等扩容操作完成节点恢复功能时刻起,到该测试节点出块、交易处理、查询等功能恢复所消耗的时间小于10min。	金融业务系统、科技产品
3	宜在30min内完成系统的节点升级	测试系统	对共识或记账节点进行应用、系统软件等升级操作完成节点恢复功能时刻起，到该测试该节点出块、交易处理、查询等功能均恢复所消耗的时间小于30min。	金融业务系统、科技产品
4	宜在30min内完成系统的节点删除	测试系统	系统中共识或记账节点下线时刻起，系统其他节点出块、交易处理、查询等功能均恢复所消耗的最长时间小于30min。	金融业务系统、科技产品
5	宜在30min内完成系统的节点增加	测试系统	系统中增加1个节点上线时刻起,到测试该节点能正常参与整个系统的出块、交易处理、查询等应用功能所消耗的时间小于30min。	金融业务系统、科技产品

7.5 账本数据增长速率

单节点数据容量增长速率性能评估内容见表60。

表60 单节点数据容量增长速率性能评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	无交易状态下账本数据增长速率应不高于声明的增长率上限、平均值	1.查看系统 2.测试系统	1.系统文档中提供无交易状态下的单节点账本数据增长速率上限说明、平均值说明。 2.实际无交易状态下的账本数据增长率不高于声明的增长速率上限。 3.实际无交易状态下的节点账本数据增长速率	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			平均值不高于声明的增长率平均值。	
2	满负载状态下账本数据增长速率应不高于声明的增长速率上限、平均值	1.查看系统 2.测试系统	1.系统提供满负载状态下的账本数据增长速率上限值、平均值说明。 2.实际满负载状态下的账本数据增长速率不高于声明的增长速率上限。 3.实际满负载状态下的节点账本数据增长速率平均值不高于声明的增长速率平均值。	金融业务系统、科技产品

8 安全性评估

8.1 基础硬件

8.1.1 基本条件

基础硬件的基本要求评估内容见表61。

表61 基础硬件的基本要求评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应遵循 GB/T 22239—2019 中三级及以上的物理和网络相关要求	1.查阅材料 2.测试系统	1.系统安全评估报告表明系统物理和网络环境符合 GB/T 22239—2019 三级及以上级别相关要求。 2.若无系统安全评估报告，系统基础硬件环境经测试符合 GB/T 22239—2019 三级及以上级别的物理和网络相关要求。	金融业务系统

8.1.2 物理安全

8.1.2.1 场地安全

场地安全评估内容见表62。

表62 场地安全评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证金融行业数据中心运行环境位于高安全区域	1.查阅材料 2.查看系统	1.项目负责人或云服务提供商说明系统位于网络安全等级保护三级及以上级别的安全物理环境中。 2.金融行业数据中心在云部署环境中位于高安全区域。	金融业务系统

8.1.2.2 硬件设备

硬件设备评估内容见表63。

表63 硬件设备评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证设备运行状态或资源使用情况异常时能发出告警	1.查阅材料 2.查看系统	1.设计文档或实施方案中包含设备运行状态和资源使用情况的监控措施，有异常情况告警机制。 2.系统监控设备能实时监控硬件设备运行状态和资源使用情况，设备运行状态或资源使用情况异常时能及时发出告警。	金融业务系统
2	应确保设备和存储介质上的数据能被清除且不可恢复	1.查阅材料 2.测试系统	1.设计文档或实施方案中包含设备和存储介质重用、报废或更换时数据清除的管理要求和技术操作要求。 2.专业数据恢复工具无法恢复设备和存储介质在重用、报废或更换时清除的数据。	金融业务系统
3	应保证不同节点使用的硬件设备具备异构性	1.查阅材料 2.查看系统	1.设计文档或实施方案包含不同节点使用两种或两种以上的硬件设备实现异构的方法。 2.系统不同节点使用的硬件设备异构的方法与设计文档或实施方案一致。	金融业务系统

8.1.2.3 节点部署安全

节点部署安全评估内容见表64。

表64 节点部署安全评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证系统关键节点冗余部署	1.查阅材料 2.查看系统	1.设计文档或实施方案包含关键节点冗余部署方案，保证任一节点故障等极端条件下系统可用性。 2.系统关键节点进行了冗余部署，与设计文档或实施方案一致。	金融业务系统
2	应保证系统承担共识或记账的节点部署在不同机房内	1.查阅材料 2.查看系统	1.设计文档或实施方案有承担共识或记账功能的节点部署说明，且明确部署在不同机房。 2.系统承担共识或记账功能的节点实际部署位置与规划方案或实施方案一致。	金融业务系统
3	应保证带有不宜共享数据的节点放置于机构内部或受保护区域	1.查阅材料 2.查看系统	1.设计文档或实施方案中包含处理或存储不宜共享数据的节点设备部署在机构内部或符合等级保护三级或更高级别要求的物理环境中的说明。 2.处理或存储不宜共享数据的节点设备部署情况与设计文档或实施方案一致，部署在机构内部或符合等级保护三级或更高级别要求的物理环境中。	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
4	应保证节点的硬件设备存储容量可扩展，避免因容量达到上限而无法同步账本	1.查阅材料 2.查看系统	1.设计文档或实施方案包含设备存储容量监测措施，以及容量达到既定阈值时的存储容量扩展方案。 2.系统可以实时监测节点设备的存储容量，当容量到达既定阈值时能及时告警。	金融业务系统

8.1.2.4 硬件加密设备安全

硬件加密设备安全评估内容见表65。

表65 硬件加密设备安全评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	硬件加密设备应经国家密码管理部门认可	查阅材料	具有国家密码管理部门颁发的硬件加密设备认证证书。	金融业务系统
2	个人密码设备应符合国家密码管理部门与行业主管部门的要求	查阅材料	有个人密码设备（如UKey、加密卡、带SE或TEE的移动终端等）的外部评估报告，符合国家密码管理部门与行业主管部门的要求。	金融业务系统

8.1.3 网络安全

8.1.3.1 网络架构安全

网络架构安全评估内容见表66。

表66 网络架构安全评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证共识节点或记账节点之间能直接进行网络通信或间接进行消息传递	1.查看系统 2.测试系统	1.系统配置文件包含共识节点或记账节点之间的网络通信配置参数。 2.经测试，共识节点或记账节点之间有通信流量，可以进行网络通信或消息传递。	金融业务系统
2	应防止单个节点故障形成网络隔离	1.查阅材料 2.查看系统	1.设计文档或实施方案中的网络拓扑结构设计合理，不存在单个节点故障网络隔离的情况，包括但不限于采用网络冗余部署等措施。 2.系统网络部署与网络拓扑结构图一致，不存在单个节点故障导致的网络隔离情况。	金融业务系统

8.1.3.2 通信传输安全

通信传输安全评估内容见表67。

表67 通信传输安全评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应在节点间建立安全传输通道	1.查阅材料 2.测试系统	1.设计文档或实施方案包含节点间建立安全传输通道的方法，包括但不限于HTTPS、VPN、加密机等方式。 2.经测试，节点间建立了安全传输通道，并且与规划方案和实施方案一致。	金融业务系统
2	应保证数据和信息能抵抗篡改、重放等主动或被动攻击	1.查阅材料 2.测试系统	1.规划方案和实施方案确使用加密、数字签名等防护措施保证数据和信息能够抵抗篡改、重放等主动或被动攻击。 2.经测试，系统采取了防篡改、防重放等保护措施，能保护数据和信息不被篡改、重放。	金融业务系统
3	应采用密码技术来保证不同节点间通信过程中敏感信息字段或整个报文的保密性	测试系统	经测试，系统通信过程中采用了密码技术对敏感信息字段或整个报文进行加密。	金融业务系统
4	可采用有权限的网络访问控制降低网络攻击造成的危害	查看系统	节点间构建了虚拟专用网络（VPN）。	金融业务系统

8.2 基础软件

8.2.1 基本条件

基础软件的基本要求评估内容见表68。

表68 基础软件的基本要求评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应符合 GB/T 22239—2019 三级及以上主机安全、应用安全、数据安全及备份恢复相关规定。	1.查阅材料 2.测试系统	1.系统评估报告表明系统基础软件符合GB/T 22239—2019三级及以上级别的主机安全、应用安全、数据安全及备份恢复相关要求。 2.若无系统安全评估报告，系统基础软件环境经测试符合GB/T 22239—2019三级及以上级别主机安全、应用安全、数据安全及备份恢复相关要求。	金融业务系统、科技产品

8.2.2 账本结构

账本结构评估内容见表69。

表69 账本结构评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	账本结构应具有防篡改性	测试系统	账本结构使用块链式或近似块链式的存储结构，并使用哈希嵌套保护数据不被篡改。	金融业务系统、科技产品
2	账本应具有数据校验功能	测试系统	账本能通过历史账本数据快速检验出被非法篡改的记录。	金融业务系统、科技产品

8.2.3 数据存储

数据存储评估内容见表70。

表70 数据存储评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应根据数据对象的类别独立存储	查阅材料	设计文档中对数据存储有规划和设计，对账户数据、交易数据、配置数据以及账本元数据等，分别存储、分别管理、分别操作。	金融业务系统、科技产品
2	应加密存储敏感信息并设置访问权限控制	1.查阅材料 2.测试系统	1.设计文档中对敏感信息的存储和使用有规划和设计，敏感信息加密存储并设置访问权限控制机制。 2.经测试，数据库中敏感信息为加密后存储，有敏感数据访问权限控制，与设计文档相关说明一致。	金融业务系统、科技产品
3	节点 CA 证书及其私钥的存储应私密管理	查阅材料	设计文档中对节点 CA 证书的管理有规划和设计，保证节点CA证书及其私钥存储的私密性。	金融业务系统、科技产品
4	数据库应选用安全高效并经过检验的主流稳定版本	查阅材料	设计文档中有系统使用的数据库型号及版本说明，并经过了选型分析和相关验证。	金融业务系统、科技产品

8.2.4 共识模块

共识模块评估内容见表71。

表71 共识模块评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应符合一致性要求	1.查阅材料 2.测试系统	1.设计文档对系统参与方参与数据打包和共识过程中共识模块协调能力有描述保证交易结果一致性的方案。 2.通过测试，所有参与共识的节点查询交易的	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			执行结果一致。	
2	应在规定时间内正确完成执行	测试系统	通过测试，系统无故障、无欺诈节点时，在规定时间内达成一致的、正确的共识，输出正确结果。	金融业务系统、科技产品
3	应在故障节点和欺诈节点数量不超过理论值的情况下系统正常工作	1.查阅材料 2.测试系统	1.设计文档中有故障节点和欺诈节点的容错阈值。 2.通过测试，系统中故障节点和欺诈节点数量不超过容错阈值时，系统能够正常工作。	金融业务系统、科技产品
4	应在故障节点和欺诈节点数量超过理论值的情况下不能达成共识	1.查阅材料 2.测试系统	1.设计文档中有故障节点和欺诈节点的容错阈值。 2.通过测试，系统中故障节点和欺诈节点数量超过容错阈值时，合法交易请求无法共识。	金融业务系统、科技产品
5	应具备“双花攻击”的防范能力	测试系统	通过测试，系统具备防范“双花攻击”的能力。	金融业务系统、科技产品

8.2.5 分布式组网

分布式组网评估内容见表 72。

表72 分布式组网评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应支持动态组网	测试系统	经测试，节点崩溃、退出以及新节点加入时，系统一致性被保留，产生的干扰不对内存服务性能产生负向影响，支持动态组网。	金融业务系统
2	应基于网络通信协议和对等网络进行通信和数据互换	1.查看系统 2.测试系统	1.系统配置文件对组网方式及相关配置说明和网络拓扑有规划和设计，节点在物理部署上进行了分离，各节点基于网络通信协议和对等网络进行通信和数据互换。 2.经测试，按照设计文档部署网络，系统能够能正确运行。	金融业务系统
3	应独立存储具有一致性的账本数据	1.查看系统 2.测试系统	1.系统配置文件各节点具有一致性的账本数据独立存储的配置。 2.经测试，各节点单个节点具有一致性的账本数据独立存储，单节点出现故障不影响整个系统正常工作。	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
4	应保证网络中无中心节点，通信控制功能应分布在各节点上，且任一节点均至少与其他两个节点建立通信连接	1.查看系统 2.测试系统	1.系统配置文件对网络节点分布有规划和设计，系统由分布在不同地点的节点互连而成。 2.经测试，网络中无中心节点，每个节点至少与其他两个节点建立了通信连接。	金融业务系统

8.2.6 智能合约

智能合约评估内容见表73。

表73 智能合约评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	宜在可信的软件/硬件支持的环境中执行	1.查阅材料 2.查看系统	1.设计文档中有智能合约运行环境规划和设计，智能合约执行环境的软件/硬件经过了安全可信评估。 2.系统中智能合约执行环境的软硬件与设计文档一致。	金融业务系统、科技产品
2	应具有智能合约访问控制机制	1.查阅材料 2.测试系统	1.设计文档对智能合约代码存储和运行有规划和设计，读取智能合约时具备相应的安全保护机制。 2.通过测试，系统禁止未授权实体读取智能合约代码与设计文档一致。	金融业务系统、科技产品
3	应具有完善的智能合约生命周期管理机制	1.查阅材料 2.测试系统	1.设计文档对智能合约生命周期管理机制有规划和设计，智能合约的存储、创建、部署、执行、冻结、解冻、注销、升级过程具有数据前向兼容能力，版本迭代时，旧版本的智能合约及时停用并存档数据，新版本智能合约可调用历史数据。 2.经测试，智能合约的存储、创建、部署、执行、冻结、解冻、注销、升级过程生命周期管理机制与设计文档一致。	金融业务系统、科技产品
4	应通过有效的智能合约审核以确保智能合约代码所表达的逻辑无漏洞	测试系统	缺陷合约特征码检测工具、智能合约自动化审计工具、基于控制流图的自动智能合约检测包、漏洞逻辑检测工具、智能合约代码级扫描器等均未检测到智能合约明显漏洞。	金融业务系统、科技产品

8.2.7 接口设计

接口设计评估内容见表74。

表74 接口设计评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	接口应隐藏底层账本的细节，为应用层提供简洁的调用方法	1.查阅材料 2.测试系统	1.设计文档对接口设计有规划，在设计接口时隐藏底层账本细节，为应用层提供简洁的调用方法。 2.经测试，监测工具截取的接口报文未显示底层账本细节，与接口设计文档一致。	金融业务系统、科技产品
2	接口应能提供交易和维护数据功能，并且有完善的权限管理机制	1.查阅材料 2.测试系统	1.设计文档对接口设计有规划，接口设计原则简洁明了，提供能够完成交易和维护数据的功能，具有完善的权限管理机制。 2.经测试，接口能够完成交易和维护数据，具有完善的权限管理机制，且与接口设计文档一致。	金融业务系统、科技产品
3	接口应具有扩展性和兼容性	查阅材料	设计文档中有接口支持扩展和兼容的设计要求，存在预留参数或预留接口。	金融业务系统、科技产品

8.2.8 数据传输

数据传输评估内容见表75。

表75 数据传输评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	数据传输时应使用SM算法对数据加密	1.查阅材料 2.测试系统	1.设计文档有数据加密传输要求，数据传输时使用对称或非对称SM算法对数据进行加密。 2.经测试，数据传输时使用SM算法对数据加密，与设计文档一致。	金融业务系统、科技产品

8.2.9 时间同步

时间同步评估内容见表76。

表76 时间同步评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证节点之间的时间戳误差维持在共识协议允许的范围内	1.查阅材料 2.查看系统	1.设计文档对时间同步有规划和设计，节点之间的时间戳误差范围有定义。 2.系统各节点时间戳误差在共识协议允许的范围内。	金融业务系统
2	应使用经过认证的中心化时间同步源进行节点间的时间	1.查阅材料 2.查看系统	1.设计文档对节点时间同步有规划和设计，有明确时间同步源要求。 2.系统时间同步源配置文件使用了经过认证	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
	同步		的中心化时间同步源进行节点间的时间同步。	

8.2.10 操作系统

操作系统评估内容见表 77。

表77 操作系统评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	系统宜支持三种及以上的操作系统或系统版本	查阅材料	设计文档有明确支持的操作系统和软件版本说明，各操作系统版本通过了系统兼容性测试。	金融业务系统、科技产品

8.3 密码算法

8.3.1 算法基本条件

8.3.1.1 对称加解密

对称加解密评估内容见表 78。

表78 对称加解密评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应采用经国家密码管理部门认可的对称加解密算法	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中含有密码设备和对称密码算法满足合规性的相关要求。 2.设计文档为开发人员提供了对称密码算法接口API，与设计文档要求一致。 3.系统配置中对称密码算法的配置参数与设计文档一致。 4.系统调用的对称加解密算法经测试与设计文档一致。	金融业务系统、科技产品
2	应验证对称加解密算法符合预期输出	1.查看系统 2.测试系统	1.系统的对称密码算法配置参数符合设计文档。 2.系统调用加密算法接口或测试相关代码的加密结果符合预期输出。	金融业务系统、科技产品
3	应验证加密算法能够支撑系统正常服务	测试系统	系统按照设计文档配置密码参数能够正常运行和提供服务。	金融业务系统、科技产品
4	应验证节点能检查出加密错误并拒绝交易	测试系统	系统在调整对称加密算法配置参数、修改接口参数、使用错误的对称加密算法等条件下，能够发现加密错误并拒绝交易。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
5	应支持可插拔的密码算法模块	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中含有支持可插拔密码算法的相关内容。 2.系统中可插拔密码算法模块的配置参数与设计文档保持一致。 3.系统更换不同的密码算法模块后，仍能继续正常提供服务。	金融业务系统、科技产品

8.3.1.2 非对称加解密

非对称加解密评估内容见表79。

表79 非对称加解密评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应采用经国家密码管理部门认可的非对称加解密算法	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中含有密码设备和非对称密码算法满足合规性的相关要求。 2.设计文档为开发人员提供了非对称密码算法接口API，与设计文档要求一致。 3.系统配置中非对称密码算法的配置参数与设计文档一致。 4.系统调用的非对称加解密算法经测试与设计文档一致。	金融业务系统、科技产品
2	应验证非对称加解密算法符合预期输出	1.查看系统 2.测试系统	1.系统的非对称密码算法配置参数符合设计文档。 2.系统调用加密算法接口或测试相关代码的加密结果符合预期输出。	金融业务系统、科技产品
3	应验证使用非对称加密算法下，用户能够正常使用系统服务	测试系统	系统按照设计文档配置密码参数能够正常运行和提供服务。	金融业务系统、科技产品
4	应验证节点能检查出非对称加密错误并拒绝交易	测试系统	系统在调整非对称加密算法配置参数、修改接口参数、使用错误的非对称加密算法等条件下，能够发现加密错误并拒绝交易。	金融业务系统、科技产品
5	应支持可插拔的密码算法模块	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中含有支持可插拔密码算法的相关内容。 2.系统中可插拔密码算法模块的配置参数与设计文档保持一致。 3.系统更换不同的密码算法模块后，仍能继续正常提供服务。	金融业务系统、科技产品

8.3.1.3 杂凑算法

杂凑算法评估内容见表80。

表80 杂凑算法评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应采用经国家密码管理部门认可的杂凑算法	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中含有密码设备和杂凑算法满足合规性的相关要求。 2.设计文档为开发人员提供了杂凑算法接口API，与设计文档要求一致。 3.系统配置中杂凑算法的配置参数与设计文档一致。 4.系统调用的杂凑算法经测试与设计文档一致。	金融业务系统、科技产品
2	应正确验证杂凑算法的内部逻辑，调用杂凑算法的接口或根据相关披露的源代码，测试摘要结果并符合预期的标准输出	1.查看系统 2.测试系统	1.系统的杂凑算法配置参数符合设计文档。 2.系统调用杂凑算法接口或测试相关代码的签名结果符合预期输出。	金融业务系统、科技产品
3	应验证使用该杂凑算法下，用户能够正常使用系统服务	测试系统	系统按照设计文档配置杂凑算法能够正常运行和提供服务。	金融业务系统、科技产品
4	宜实现可插拔式杂凑算法	1.查阅材料 2.查看系统 3.测试系统	1.设计文档中含有支持可插拔密码算法的相关内容。 2.系统中可插拔密码算法模块的配置参数与设计文档保持一致。 3.系统更换不同的密码算法模块后，仍能继续正常提供服务。	金融业务系统、科技产品

8.3.1.4 随机数

随机数评估内容见表81。

表81 随机数评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应采用经国家密码管理部门认可的随机数算法	1.查阅材料 2.测试系统	1.设计文档中描述了随机数算法或设备，且具有算法经过国家密码管理部门认可的信息。 2.系统测试产生的随机数符合 GB/T 32915 的规定，与设计文档一致。	金融业务系统、科技产品

8.3.2 保密性

保密性评估内容见表82。

表82 保密性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保障敏感信息的保密性	1.查阅材料 2.查看系统 3.测试系统	1.设计文档包含在交换敏感信息时的会话初始化过程设计，并设计完整的机制，保证在通信过程中使用密钥交换算法协商会话密钥，保护敏感信息。 2.系统中网络和主机的会话密钥的建立和使用符合设计文档。 3.测试系统建立敏感信息的通信，计算报文的加密数据，该数据符合预期。	金融业务系统、科技产品

8.3.3 完整性

完整性评估内容见表83。

表83 完整性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保障敏感信息的完整性	1.查阅材料 2.查看系统 3.测试系统	1.设计文档对关键数据在传输和存储中的完整性，并在对数据处理前检验其完整性，进行了说明。 2.系统中网络和主机的关键数据传输和存储过程中完整性符合设计文档。 3.测试系统建立敏感信息的通信，计算报文的完整性数据，该数据符合预期。	金融业务系统、科技产品

8.3.4 真实性

真实性评估内容见表84。

表84 真实性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保障实体的真实性	1.查阅材料 2.测试系统	1.设计文档中明确设计了使用非对称加密、动态口令或数字签名等方式保障真实性。 2.设计文档设计的真实性应用场景包括：进入重要物理区域人员、节点通讯双方、网络设备接入时、登录操作系统和数据库系统。 3.测试系统分别针对以上场景的真实性身份鉴别进行测试验证，验证结果符合设计文档。	金融业务系统、科技产品

8.4 节点通信

8.4.1 节点身份验证

节点身份验证评估内容见表 85。

表85 节点身份验证评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应在节点接入时进行合法身份认证	查看系统	系统日志记录了节点接入时合法身份认证过程，认证为合法身份的节点允许加入系统。	金融业务系统、科技产品
2	应在节点接入时进行非法身份认证	查看系统	系统日志记录了节点接入时非法身份认证过程，认证为非法身份的节点拒绝加入系统。	金融业务系统、科技产品
3	应在节点通讯时进行身份双方认证	查看系统	系统日志或者程序代码描述了双方节点身份认证过程。	金融业务系统、科技产品
4	应在节点通讯身份双方认证时采用加密技术	1.查阅材料 2.测试系统	1.设计文档包含节点身份认证的加密机制和加密算法相关说明，采用的加密技术符合国家密码管理部门的要求。 2.节点身份认证的通信报文采用加密机制和加密算法进行加密，采用的加密技术与设计文档描述一致。	金融业务系统、科技产品

8.4.2 通信完整性

通信完整性评估内容见表 86。

表86 通信完整性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应采用经国家密码管理部门认可的消息鉴别码算法、数字签名等密码技术校验数据传输的完整性	1.查阅材料 2.查看系统	1.设计文档包含校验数据传输完整性的消息鉴别码算法、数字签名等密码技术的说明，采用的密码技术符合国家密码管理部门的要求。 2.节点通信报文采用国家密码标准的消息鉴别码算法、数字签名等密码技术校验数据传输完整性，与设计文档描述一致。	金融业务系统、科技产品
2	应保证通讯节点中的通讯链路数据完整性	1.查阅材料 2.测试系统	1.设计文档包含保证通讯节点中的通讯链路数据完整性等技术措施。 2.系统模拟的异常请求包在接收端异常，说明节点间通讯链路中具有数据完整性校验过程。	金融业务系统、科技产品
3	在节点通讯网络异常时，服务应具备异常处理机制	1.查阅材料 2.测试系统	1.设计文档包含节点通讯网络异常情况的服务异常处理机制。 2.系统提供了对网络丢包、抖动、延时等网络通讯异常情况下的异常处理机制，与设计文档描述一致。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
4	当节点通讯网络断网时，节点通讯应具备断网重连机制	1.查阅材料 2.测试系统	1.设计文档包含节点通讯网络断网时的断网重连机制。 2.系统提供节点通讯网络断网的断网重连机制，与设计文档描述一致。	金融业务系统、科技产品

8.4.3 通信保密性

通信保密性评估内容见表87。

表87 通信保密性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	节点进行数据通讯整个过程中，报文或会话应经过加密处理	1.查阅材料 2.查看系统	1.设计文档包含节点间通信报文或会话的加密机制和加密算法的说明，采用的加密技术符合国家密码管理部门的要求。 2.节点通信报文或会话进行了加密处理，其加密机制和加密算法与设计文档描述一致。	金融业务系统、科技产品
2	节点通讯应采用符合国家密码管理部门要求的技术建立安全通信通道	1.查阅材料 2.查看系统	1.设计文档包含节点通讯所建立的安全通信通道的说明，采用的加密技术符合国家密码管理部门的要求。 2.系统建立的安全通信通道（如TLS）版本符合当前通信安全规范。若涉及境外业务、境外服务器、境外主体机构则本项不适用。	金融业务系统、科技产品

8.5 账本数据

8.5.1 账本数据完整性

账本数据完整性评估内容见表88。

表88 账本数据完整性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证账本数据生成的完整性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对账本数据生成操作的权限管理机制和相关设计进行了说明。 2.与安全专员确认有支撑账本数据生成操作不被非授权方式更改或破坏的手段。 3.系统提供措施支持账本数据的生成操作不可被非授权方式更改或破坏。 4.经测试，系统具备账本数据生成时的完整性校验功能，并在检测到数据生成的完整性被破坏时能够进行报警。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
2	应保证账本数据传输的完整性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对账本数据传输完整性检测的相关设计进行了说明。 2.与安全专员确认有支撑账本数据传输操作不被非授权方式更改或破坏的手段。 3.系统提供措施支持账本数据的传输操作不可被非授权方式更改或破坏。 4.经测试，系统具备账本数据传输时的完整性校验功能，并在检测到数据传输的完整性被破坏时能够进行报警。	金融业务系统、科技产品
3	应保证账本数据存储的完整性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对账本数据存储机制及其存储保密性设计、账本数据存储管理配置项设计、数据存储完整性检测及在检测到完整性错误时采取恢复措施的设计进行了说明。 2.与安全专员确认有实现账本数据存储机制设计、账本数据存储保密性设计、账本数据存储管理可选配置项及数据存储完整性检测的手段。 3.系统实际提供措施支持账本数据的存储保密性、存储管理配置项的选择、账本数据的存储操作不可被非授权方式更改或破坏、非特殊情况下账本信息不被删除等功能，账本数据依据相关设计实现了保密存储，数据删除等操作实现了日志留存，留存期限符合国家有关规定。 4.经测试，系统能实现账本数据的保密存储，具备检测到账本数据在存储过程中完整性受到破坏、账本数据在存储过程中被非授权方式更改或破坏的功能，实现了对账本数据的完整性校验并在检测到数据完整性被破坏时进行报警，在检测到完整性错误时能采取措施进行恢复。	金融业务系统、科技产品
4	应保证账本数据调用的完整性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对使用的接口进行权限管理设计和数据调用的完整性设计进行了说明。 2.与安全专员确认依据账本数据类别（如关键业务数据、敏感数据、一般数据）形成了关于调用、查看等操作的权限管理，具备支撑权限管理要求、防止未授权调用的手段。 3.系统提供针对账本数据调用等操作的权限配置，能支持账本数据的调用操作不可被非授权方式更改或破坏并防止未授权的调用。 4.经测试，系统能实现未被授权调用敏感数据	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			的账号无法进行敏感数据调用操作和被授权可调用敏感数据的高权限系统账号能够进行权限内的账本敏感数据调用操作，调用操作的行为均被写入了日志。	

8.5.2 账本数据一致性

账本数据一致性评估内容见表 89。

表89 账本数据一致性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证记账节点的账本数据写入的一致性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对账本数据写入一致性的共识策略和一致性算法的设计进行了说明。 2.经与安全专员确认，系统具有确保账本数据写入一致性的共识策略和一致性算法的设计。 3.系统具备支撑共识算法和一致性算法的方法和手段，具备保证账本数据写入一致性的方法和手段。 4.经测试，系统各记账节点存储的账本数据实现基于共识的写入一致性，能支持合规的交易数据依据共识算法和一致性算法在各记账节点写入和同步，不合规交易数据被拒绝写入账本。	金融业务系统、科技产品
2	应保证账本数据修改的一致性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对确保账本数据修改一致性的共识策略和一致性算法的设计进行了说明。 2.经与安全专员确认，系统具有账本数据修改一致性的共识策略和算法设计。 3.系统具备支撑共识算法和一致性算法的方法和手段，具备保证账本数据修改一致性的方法和手段。 4.经测试，节点之间采取技术手段对接收的数据进行鉴别，防止数据被修改、伪造；系统各记账节点存储的账本数据实现基于共识的修改一致性，能支撑实现合规的交易数据依据共识算法和一致性算法在各记账节点修改和同步，不合规的修改数据被拒绝写入账本。	金融业务系统、科技产品
3	应保证账本数据存储的一致性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对账本数据存储一致性的共识策略和算法设计以及节点与系统断开连接或被攻击情况下的数据存储一致性保障策略设计进行了说明。 2.经与安全专员确认，系统具有确保账本数据	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			存储一致性的共识策略和算法设计以及节点与系统断开连接或被攻击情况下的数据存储一致性保障策略设计。 3.系统具备支撑共识算法和一致性算法的方法和手段，具备保证账本数据存储一致性的方法和手段；在攻击行为导致数据被污染时，系统能提供相关手段支持被攻击节点可通过与其他可信节点交互等方式来检测出攻击及数据污染的发生，能对数据被污染的情况及时响应。 4.经测试，新节点能同步和下载权限范围内的账本数据并确保下载的结果正确；记账节点与系统断开连接，再次恢复连接后，该记账节点能保持和正常节点间账本数据的一致性，能同步和下载权限范围内的账本数据并确保下载的结果正确。	

8.5.3 账本数据保密性

账本数据保密性评估内容见表90。

表90 账本数据保密性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证账本数据传输的保密性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对敏感数据的界定和分类及其账本数据传输保密性设计进行了说明，采用的加密算法符合国家密码管理部门的要求。 2.经与安全专员确认，系统具有账本数据传输保密性设计，与设计文档中所描述一致。 3.系统实际提供措施供用户实现敏感数据的传输保密性。 4.经测试，未经授权的节点无法请求获取敏感数据并获取操作有认证检查环节；系统对账本数据进行加密传输，在传输时对数据加密的密钥和证书采用与信息传输不同的传输通路进行传递。	金融业务系统、科技产品
2	应保证账本数据存储的保密性	1.查阅材料 2.访谈人员 3.查看系统	1.设计文档对敏感数据的界定和分类及其账本数据存储保密性设计进行了说明，采用的加密算法符合国家密码管理部门的要求。 2.经与安全专员确认，系统包含账本数据存储保密性设计，与设计文档中所描述一致。 3.系统实现账本敏感数据的加密存储。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
3	账本数据中敏感数据的保护密钥和账本数据本身应分开保存，并且保护密钥应支持存放在安全的密码模块中	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对账本敏感数据保护密钥的保存策略设计进行了说明，并明确规定保护密钥和账本数据本身分开保存，保护密钥存放在安全的密码模块中。 2.经与安全专员确认，系统包含账本敏感数据保护密钥的保存策略设计，与设计文档中所描述一致。 3.系统实现保护密钥与账本数据分开保存，保护密钥存放在安全的密码模块中。 4.经测试，系统能提供密钥挂失、密码重置、密钥丢失后签名保护和资产锁定等功能。	金融业务系统、科技产品

8.5.4 账本数据有效性

账本数据有效性评估内容见表91。

表91 账本数据有效性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应能够对节点存储的账本数据有效性进行校验	1.查阅材料 2.访谈人员 3.测试系统	1.设计文档对系统支持的共识协议和算法列表进行了说明。 2.经与安全专员确认，系统所支持的共识协议和算法列表与设计文档一致。 3.经测试，记账节点对账本数据的存储符合列表内的共识协议和算法。	金融业务系统、科技产品
2	应使用符合“共识协议”章节中要求共识协议保证账本数据的有效性	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对节点存储的账本数据进行有效性校验的规则设计进行了说明，并规定在某一节点或多节点账本数据失效情况下采用共识协议以保证账本数据的有效性。 2.与安全专员确认系统账本数据的有效性所采用的共识协议与设计文档一致。 3.系统能提供相应手段支撑对账本数据有效性进行校验，保证数据结构、语法规范性、输入输出和数字签名等方面符合设计要求；系统能提供实用拜占庭容错及类似实用拜占庭容错功能，确保系统在一定数量的恶意节点存在下仍能正常运行。 4.经测试，停掉相应数量的记账节点之后，系统网络依然能够依据账本采用的共识协议正确执行交易、达成共识并记账，被停掉的节点恢复后能够自动同步最新账本；停掉某一记账	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			节点，在系统设计的时间内能够恢复，并自动同步最新账本并恢复记账能力。	

8.5.5 账本数据冗余

账本数据冗余评估内容见表92。

表92 账本数据冗余评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应能防止因单个节点失效而造成总账本数据的丢失	1.查阅材料 2.访谈人员 3.查看系统	1.设计文档对账本数据在系统中的冗余性设计进行了说明，能防止因单个节点失效而造成总账本数据的丢失。 2.经与安全专员确认，系统实现了账本数据冗余性设计。 3.系统提供账本数据（尤其是重要数据）的冗余性存储以及备份恢复功能。	金融业务系统、科技产品

8.5.6 账本数据访问与使用

账本数据访问与使用评估内容见表93。

表93 账本数据访问与使用评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	账本数据访问与使用符应合认证授权要求	1.查阅材料 2.访谈人员 3.测试系统	1.设计文档对账本数据授权和验证的设计、账本数据中个人信息等数据进行访问与使用时的隐私保护措施进行了说明,符合认证授权要求。 2.经与安全专员确认提供的账本数据访问与使用认证授权措施。 3.经测试，系统能够为创建的账号分配账本数据权限；登录系统访问权限范围内的账本数据时有验证信息；登录系统访问权限范围外的账本数据时访问失败，提示没有访问权限；系统在对客户个人信息及由信息加工后产生的信息进行展示时，对客户身份标识信息进行了部分隐藏，非密文展示采取了去标识化措施；在对非本人展示相关信息及由信息加工后产生的信息时，获得了信息所有者的授权，并对展示人进行了认证；针对客户提供了信息备份和导出的手段，备份和导出的信息经过了加密处理并给客户提供了解密手段；对客户提供了信息注	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
			销不可见的手段，信息注销不可见时获得了客户认证和授权；对于敏感交易，系统提供技术手段由特定许可实体进行验证或背书。	
2	账本数据的访问与使用应满足访问控制要求	1.查阅材料 2.访谈人员 3.查看系统 4.测试系统	1.设计文档对账本数据针对单一应用调用和跨应用调用有不同级别、不同分类的账户访问权限和安全策略设计进行了说明。 2.经与安全专员确认系统提供账本数据访问与使用访问控制措施。 3.系统提供满足访问控制要求的技术手段或措施对账本数据的访问与使用进行控制。 4.经测试，针对单一应用调用，匿名用户无法操作账本数据，不同用户间无法越权操作账本数据；针对跨应用调用，匿名错误的应用鉴别信息无法调用应用提供的接口，权限不同的应用鉴别信息，无法成功调用非其权限内的应用接口；系统能提供账户权限的变更和授权，不同账户之间进行授权支持有效时间的设定。	金融业务系统

8.5.7 账本数据安全审计

账本数据安全审计评估内容见表94。

表94 账本数据安全审计评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	账本数据访问应提供安全审计功能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档对账本数据的访问安全审计功能设计进行了说明，审计记录包括访问的日期、时间、用户标识、数据内容等审计相关信息。 2.系统提供账本数据的访问安全审计功能并具备保护审计进程的措施，定义审计跟踪极限的阈值，审计日志留存时间满足国家及行业监管部门要求；根据信息系统的统一安全策略实现集中审计，时钟保持与时钟服务器同步。 3.经测试，系统启用的账本数据访问安全审计功能有效，审计记录完整。	金融业务系统
2	数据变更应提供审计功能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档对账本数据的变更安全审计功能设计进行了说明，审计记录包括数据变更成功的记录，数据变更失败的记录。 2.系统提供账本数据变更的安全审计功能并具备保护审计进程的措施，定义审计跟踪极限的阈值，审计日志留存时间满足国家及行业监管部门要求；根据信息系统的统一安全策略实现	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
			集中审计，时钟保持与时钟服务器同步。 3.经测试，系统启用的数据变更安全审计功能有效，审计记录完整。	
3	节点有效性校验失败、一致性校验失败等情况下同步账本数据，应提供安全审计功能	1.查阅材料 2.查看系统 3.测试系统	1.设计文档对节点有效性校验失败、一致性校验失败等情况下同步账本数据的安全审计功能设计进行了说明，审计记录包括事件类型、原因、账本数据同步的节点、账本数据校验值等审计相关信息。 2.系统提供对节点有效性校验失败、一致性校验失败等情况下同步账本数据的安全审计功能并具备保护审计进程的措施，定义审计跟踪极限的阈值，审计日志留存时间满足国家及行业监管部门要求；根据信息系统的统一安全策略实现集中审计，时钟保持与时钟服务器同步。 3.经测试，系统启用的对节点有效性校验失败、一致性校验失败等情况下同步账本数据的安全审计功能有效，审计记录完整。	金融业务系统

8.6 共识协议

8.6.1 合法性

共识协议合法性评估内容见表95。

表95 共识协议合法性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应确保参与共识过程的节点经过验证	1.查看系统 2.测试系统	1.系统日志对节点 ID 与节点实体的一一对应进行了说明。 2.经测试，节点的加入和退出操作能够通过合法性验证。	金融业务系统、科技产品

8.6.2 正确性

共识协议正确性评估内容见表96。

表96 共识协议正确性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	共识协议依据的算法理论应公开或经过安全评估	查阅材料	共识协议依据的算法理论是公开发表的或具有安全评估报告，修改后的共识协议经过了同行评议。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
2	协议算法的测试应全面完整，宜应用形式化验证或进行代码审计以确保算法实现的正确性	查阅材料	1.具有共识协议算法形式化验证和代码审计报告。 2.审计报告中所验证的共识算法包括但不限于工作量证明、权益证明、实用拜占庭容错算法或其他分布式系统一致性算法。 3.审计报告中所验证的共识算法，能够保证依据该算法实现的账本状态的正确性和一致性。	金融业务系统、科技产品
3	可信节点应为协议算法的运行提供安全可信的硬件软件基础	1.查阅材料 2.查看系统	1.设计文档中列出所部署的硬件软件（如服务器、操作系统等）基础是安全可信的。 2.在生产环境中支撑节点运行的硬件软件（如服务器、操作系统等）基础安全可信，与设计文档中一致。	金融业务系统

8.6.3 终局性

共识协议终局性评估内容见表 97。

表97 共识协议终局性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	算法应在可接受的有限时间内具有终局性	测试系统	经测试，所有参与共识的可信节点，在系统设计文档规定的可接受时间范围内，最终能够达成一致性结果。	金融业务系统、科技产品

8.6.4 不可伪造性

共识协议不可伪造性评估内容见表 98。

表98 共识协议不可伪造性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	任何对系统当前状态进行恶意构造以欺骗其他可信节点所需要的时间，应不少于可接受范围	1.查阅材料 2.测试系统	1.设计文档声明了共识算法容错率，若采用工作量证明时该比例为 50%。 2.经测试，在系统中配置恶意节点占比不超过共识协议容错率时，所进行任何对系统当前状态进行恶意构造以欺骗其他可信节点所需要的时间在系统设计文档规定的不可接受范围内。	金融业务系统、科技产品

8.6.5 健壮性

共识协议健壮性评估内容见表 99。

表99 共识协议健壮性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	被攻击节点应通过与系统中其他可信节点交互等方式来检测出攻击及数据污染的发生	测试系统	经测试，系统遭受网络故障或账本被删除或遭到恶意篡改等攻击后，数据不会丢失；恢复连接后，节点数据能够恢复正常状态且保持和正常节点间数据的一致性。	金融业务系统、科技产品

8.6.6 低延时

共识协议低延时评估内容见表 100。

表100 共识协议低延时评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	共识协议应保持低响应延迟	测试系统	经测试，在当前共识协议配置下执行交易，参与的节点交易达成共识所需平均时间满足金融系统对于数据同步的时间要求。	金融业务系统

8.6.7 激励相容

共识协议激励相容评估内容见表 101。

表101 共识协议激励相容评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应采用激励机制保障系统安全	查看系统	系统采用激励机制来保障系统的运行安全，在系统上运行应用的激励价值不超过系统的安全阈值。	金融业务系统

8.6.8 可监管性

共识协议可监管性评估内容见表 102。

表102 共识协议可监管性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	单次共识过程和系统运行的整个生命周期都应可审计、可监管	1.查阅材料 2.查看系统	1.设计文档包含对留存的日志文件类型、留存手段和留存期限的说明，留存期限满足国家及行业监管部门要求。 2.系统能够提供证明安全追溯需要的材料和相应的文档记录，如运维人员操作记录、安全审计报告、安全事件处理流程记录、安全事故处理报告、关键组件运行日志等信息。	金融业务系统、科技产品（若未提供审计功能则不适用）

序号	实现要求	评估方法	结果判定	适用对象
			3.系统日志、节点间的通信日志以及账本变更历史等日志中记录了单次共识过程和系统运行的整个共识过程；关键系统日志及账本进行定期备份或进行冗余性处理。	

8.7 智能合约

8.7.1 访问控制

智能合约访问控制评估内容见表103。

表103 智能合约访问控制评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供用户访问智能合约的控制机制	1.查阅材料 2.测试系统	1.设计文档对用户访问智能合约的控制机制有规划和设计。 2.系统支持先确认用户身份，并配置相关的控制机制，对用户访问智能合约进行控制。	金融业务系统、科技产品
2	应提供智能合约之间相互访问的控制机制	1.查阅材料 2.测试系统	1.设计文档对智能合约之间相互访问的控制机制有规划和设计，支持智能合约之间相互访问，并具备安全访问控制手段。 2.系统支持智能合约之间相互访问，并具备安全访问控制手段。	金融业务系统、科技产品
3	应提供智能合约访问外部数据的控制机制	1.查阅材料 2.测试系统	1.设计文档对智能合约访问外部数据的控制机制有规划和设计，支持智能合约访问外部数据，并具备安全访问控制手段。 2.系统支持智能合约访问外部数据，并具备安全访问控制手段。	金融业务系统、科技产品
4	应对智能合约提供隔离的执行环境	1.查阅材料 2.测试系统	1.设计文档对智能合约的隔离的执行环境有规划和设计。 2.系统支持智能合约在隔离的执行环境运行。	金融业务系统、科技产品

8.7.2 原子性

智能合约原子性评估内容见表104。

表104 智能合约原子性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	智能合约的执行应有原子性	测试系统	系统将智能合约的一组业务操作组成一个原子单元，只有当单元内所有操作都执行成功时，交易才能成功，否则单元内的所有操作都将回滚。	金融业务系统、科技产品

8.7.3 安全审计

智能合约安全审计评估内容见表105。

表105 智能合约安全审计评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	智能合约应经过相关专业技术人员的审计，并保留审计记录	查阅材料	设计文档对智能合约的安全审计和评估对象进行了说明，包括智能合约设计及业务逻辑安全、源代码安全审计、编译环境审计及相关的应急响应等；可提供经过相关专业技术人员审计的智能合约审计报告。	金融业务系统、科技产品

8.7.4 攻击防范

智能合约攻击防范评估内容见表106。

表106 智能合约攻击防范评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	系统应能够对抗由智能合约引起的DDoS攻击等	查看系统	系统提供相应机制保证能够对抗由智能合约引起的DDoS攻击，防止其长时间占用资源。	金融业务系统、科技产品
2	应具备在遭受DDoS攻击等影响下干预智能合约运行的机制	查看系统	系统提供相应机制保障在系统遭受DDoS攻击、服务受到影响时，智能合约的运行可被干预。	金融业务系统、科技产品
3	应有相应机制防止隔离执行环境中的智能合约访问其执行环境之外的资源	查看系统	系统提供相应机制防止隔离执行环境中的智能合约访问其执行环境之外的资源。	金融业务系统、科技产品

8.7.5 安全验证

智能合约安全验证评估内容见表107。

表107 智能合约安全验证评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应基于智能合约安全规则库和问题合约模式库实现智能合约的漏洞检测	1.查阅材料 2.查看系统	1.漏洞检测报告使用了基于智能合约安全规则库和问题合约模式库进行漏洞检测的机制。 2.系统中所部署的漏洞检测系统提供的安全扫描包括智能合约源码和字节码两方面。	金融业务系统、科技产品
2	应实现基于安全规则和配置信息自动	1.查阅材料 2.查看系统	1.设计文档对基于安全规则和配置信息自动生成安全智能合约模板的机制进行了说明。	金融业务系统、科

序号	实现要求	评估方法	结果判定	适用对象
	生成安全智能合约模板的机制		2.系统智能合约的安全验证是基于安全规则和配置信息自动生成智能合约模板机制。	技产品

8.8 身份管理

8.8.1 身份注册

身份注册评估内容如下表108。

表108 身份注册评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备身份注册的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中包含身份生命周期的管理规章制度和信息系统，并对身份注册信息的收集、使用、存储、传输、销毁等过程有明确说明，符合相关法律法规要求。 2.系统身份注册流程经测试符合设计要求。	金融业务系统

8.8.2 身份核实

身份核实评估内容见表109。

表109 身份核实评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备身份核实的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了注册机构核实注册实体身份、完善核实管理制度、避免单人完成操作、具备材料核验的技术手段、接受监管审计的要求。 2.系统身份核实流程经测试符合设计要求。	金融业务系统

8.8.3 账户管理

账户管理评估内容见表110。

表110 账户管理评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备账户创建的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了身份标识具有全局唯一性、隐私匿名性、账户身份分级、账户权限管理的要求。 2.系统账户创建流程经测试符合设计要求。	金融业务系统
2	应具备账户授权的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了普通账户和特殊账户的授权流程，普通账户独立完成授权，	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
			特殊账户由各参与方共识授权。 2.系统账户授权流程经测试符合设计要求。	
3	应具备凭证签发的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了颁发身份凭证必须通过权威机构对实名登记信息进行核验的要求。 2.系统凭证签发流程经测试符合设计要求。	金融业务系统
4	应具备账户冻结和解冻的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了账户冻结和解冻的要求，账户冻结由注册机构发起，经共识后修改账户状态为冻结，冻结的账户不能进行交易；账户解冻由注册机构发起，达成共识解冻后的账户可继续进行交易。 2.系统账户冻结和解冻流程经测试符合设计要求。	金融业务系统
5	应具备账户锁定和恢复的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定账户锁定和恢复的流程，防止恶意的私钥重置。 2.系统账户锁定和恢复流程经测试符合设计要求。	金融业务系统
6	应具备账户注销的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了账户应设定使用期限、注销申请功能、定期发布公开和可查询账户注销列表功能、重置公私钥对功能和已注销账户的管理功能。 2.系统账户注销流程经测试符合设计要求。	金融业务系统

8.8.4 凭证生命周期管理

凭证生命周期管理评估内容见表111。

表111 凭证生命周期管理评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备凭证生命周期管理的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中包括凭证的生产、存储、使用、撤销、终止整个过程，规定了用户身份凭证类型、内容、操作可追溯、防伪机制与管理措施。 2.系统凭证生命周期管理流程经测试符合设计要求。	金融业务系统
2	应具备凭证产生的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了凭证产生过程，用户向凭证提供方发起凭证申请，凭证提供方对用户进行身份核验，通过身份核验后，凭证提供方生成带有数字签名的凭证发放给用户。 2.系统凭证产生流程经测试符合设计要求。	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
3	应具备凭证发放的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了凭证发放流程，由身份注册机构保证数字身份凭证的私有部分的安全传输和不被第三方窃取。 2.系统凭证发放流程经测试符合设计要求。	金融业务系统
4	应具备凭证存储的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了凭证安全存储，隐私保护，实现机制和持久性存储的目的、方法和位置。 2.系统凭证存储过程经测试符合设计要求。	金融业务系统
5	应具备凭证流转的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了凭证流转流程，凭证流转由用户发起，对凭证信息的访问必须经过用户授权许可。 2.系统凭证流转流程经测试符合设计要求。	金融业务系统
6	应具备凭证验证的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了凭证验证流程，凭证支持基于密码算法的验真功能，凭证需求方可对用户提交的凭证进行真实性验证。 2.系统凭证验证流程经测试符合设计要求。	金融业务系统
7	应具备凭证更新的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定凭证更新流程，凭证到期之前采取安全快捷的方式确保用户凭证重新生效，建立保障机制确保用户数字身份属性值及时更新，变更属性核实后进行更新登记，结果反馈给用户完成更新流程。 2.系统凭证更新流程经测试符合设计要求。	金融业务系统
8	应具备凭证终止的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了凭证的有效期限和凭证到期自动失效。 2.系统凭证终止流程经测试符合设计要求。	金融业务系统

8.8.5 身份鉴别

身份鉴别评估内容见表112。

表112 身份鉴别评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备身份鉴别的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了提供专门的组件或模块实现用户身份认证功能。 2.设计文档、管理文档中规定了使用经国家密码管理部门认可的算法和协议对通讯双方的身份进行认证，对重要数据、业务或系统的操作采用双因素身份认证，并确保用户口令等身份认证相关凭证信息的存储安全性。 3.设计文档、管理文档中规定了定期对用户账号的使用情况进行安全性分析，并评估账号的	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
			安全风险，并具有认证失败处理机制。 4.测试系统验证身份鉴别流程符合设计要求。	

8.8.6 节点标识管理

节点标识管理评估内容见表113。

表113 节点标识管理评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备节点标识管理的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了节点授权机构及管理员。 2.设计文档、管理文档中规定了通信节点加入系统之前，由授权机构给予其在系统内唯一的节点标识，并具有不易被仿冒的特点。 3.设计文档、管理文档中规定了节点之间建立数据通信连接之前，通过标识鉴别信息实现双向身份认证，并建立一条安全的数据通信信道，确保保密性和完整性。 4.设计文档、管理文档中规定了节点标识认证失败时的处理机制。 5.系统节点标识管理功能经测试符合设计要求。	金融业务系统

8.8.7 身份更新和撤销

身份更新和撤销评估内容见表114。

表114 身份更新和撤销评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备身份更新和撤销的功能	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定了实体对身份信息进行更新和撤销的流程。 2.测试系统验证身份更新和撤销符合设计要求。	金融业务系统

8.8.8 身份信息安全性

身份信息安全性评估内容见表115。

表115 身份信息安全性评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保障身份信息的安全性	1.查阅材料 2.测试系统	1.自查报告、审计报告、外部评估报告等证明材料中身份信息安全符合 JR/T 0171—2020 规定。 2.设计文档中包括了身份数据保密机制的设计，基于属性的访问控制的设计，隐私保护要求的设计，合规性、认证和审计的策略。 3.系统身份信息安全鉴别流程经测试符合设计要求。	金融业务系统
2	应保障身份信息的密钥安全性	1.查阅材料 2.查看系统 3.测试系统	1.设计文档、管理文档说明了身份密钥的类型及生命周期管理。 2.密钥管理系统具有管理密钥安全性、创建、派生、分发、存储和其他管理安全审计功能。 3.系统用户身份密钥符合金融市场所需安全要求的加密算法及密钥长度。 4.系统对用户丢失密钥、密钥过期或受到其他危害时提供密钥轮换、销毁和替换的方法。	金融业务系统
3	应保障身份信息安全加密	1.查阅材料 2.测试系统	1.设计文档、管理文档中规定密码算法符合国家密码管理部门要求。 2.系统信息安全加密符合设计要求。	金融业务系统

8.8.9 身份监管审计

身份监管审计要求评估内容见表 116。

表116 身份监管审计评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备客户监管信息的方法和手段，并严格审批和使用监管权限	1.查阅材料 2.查看系统	1.设计文档规定了监管信息的内容，提供收集客户监管信息的方法和手段，明确信息监管的目标、方式、范围、规则等。 2.系统严格审批和使用监管权限，除特殊情况外，监管部门应取得授权。	金融业务系统
2	应对身份、账户、凭证的访问和更改提供安全审计功能	查看系统	1.系统具备安全审计功能，审计记录包括访问的日期、时间、用户标识、数据等相关信息。 2.系统身份生命周期管理中通过共识机制完成的业务流程，审计记录包括策略、共识节点、账本数据校验值等相关信息。	金融业务系统

8.9 隐私保护

8.9.1 隐私保护策略

隐私保护策略评估内容见表 117。

表117 隐私保护策略评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应根据具体使用场景制定相关的隐私保护策略，平衡信息保密性、隐私保护程度与执行效率间的制约关系	1.查阅材料 2.查看系统	1.设计文档说明了不同使用场景及其对应的隐私保护策略，包括但不限于信息公开可验证、信息加密可验证和信息由交易验证节点验证等。 2.系统能根据不同的业务类型，配置不同的隐私保护策略。	金融业务系统

8.9.2 隐私保护技术

隐私保护技术要求评估内容见表 118。

表118 隐私保护技术要求评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保障信息采集时的隐私安全	1.查阅材料 2.查看系统 3.测试系统	1.设计文档说明了个人信息采集的最小化设计原则；获取个人信息的途径和类别；收集信息的目的和处理方式、存储期限、智能合约逻辑内容；用户自主选择同意或拒绝的操作步骤；对采集的信息进行匹配认证等。 2.系统的数据采集配置符合设计文档要求。 3.系统的数据采集过程经测试符合设计文档要求。	金融业务系统、科技产品
2	应保障信息传输时的隐私安全	1.查阅材料 2.查看系统 3.测试系统	1.设计文档说明了信息传输时全量加密的策略，加密密钥和证书安全传输的策略。 2.系统的数据传输配置符合设计文档要求。 3.系统的数据传输过程经测试符合设计文档要求。	金融业务系统、科技产品
3	应保障信息存储时的隐私安全	1.查阅材料 2.查看系统 3.测试系统	1.设计文档说明了与个人信息敏感级别相对应的存储安全策略，包括对高敏感级别个人信息使用不可逆密码算法加密存储，对中低敏感级别个人信息采用加密存储；信息存储时对客户身份标识信息进行摘要存储；信息在第三方存储时告知客户并获得客户授权的方式。 2.系统的数据存储配置符合设计文档要求。 3.系统的数据存储过程经测试符合设计文档要求。	金融业务系统、科技产品
4	应保障信息使用时的隐私安全	1.查阅材料 2.查看系统	1.设计文档、管理文档说明了隐私信息使用时，记录使用者、使用内容、使用频率的要求；用户信息展示的安全策略，包含对展示的客户身份标识信息进行部分隐藏；非密文展示采取	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			去标识化措施；非本人展示先获得信息所有者的授权等。 2.系统的数据使用配置符合设计文档要求。 3.系统信息展示过程经测试符合设计文档要求。	
5	应保障信息销毁时的隐私安全	1.查阅材料 2.查看系统 3.测试系统	1.设计文档说明了客户隐私信息销毁过程的安全保护策略，包含向客户提供信息备份和导出的手段；信息注销不可见时获得客户认证和授权等。 2.系统的信息销毁配置符合设计文档要求。 3.系统的信息销毁过程经测试符合设计文档要求。	金融业务系统、科技产品

8.9.3 隐私保护监控与审计

隐私保护监控与审计评估内容见表119。

表119 隐私保护监控与审计评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应制定完备的隐私保护审计方案	1.查阅材料 2.查看系统	1.设计文档对审计方案进行了说明，审计内容包括隐私保护策略和隐私保护技术手段，审查形式包括但不限于日常监控、定期审计、不定期审计。 2.系统配置中开启了隐私保护的监控和审计。	金融业务系统
2	应审查所制定的隐私保护策略和隐私保护技术手段的合理性	查看系统	系统的信息管理遵循了隐私保护原则，对不同隐私保护等级的金融信息采取了相应的风险防范措施。	金融业务系统
3	应审查隐私保护策略和隐私保护技术手段的执行过程和执行效果	1.查阅材料 2.查看系统	1.操作手册、操作记录等支持性文档记录了隐私保护策略和隐私保护技术手段的执行过程。 2.系统具有隐私保护执行过程监控、审计策略的配置，并有审计日志。	金融业务系统
4	应在必要时对隐私保护策略和隐私保护技术手段进行更新	1.查阅材料 2.查看系统	1.设计文档设计包含隐私保护策略和隐私保护技术手段更新的步骤。 2.系统隐私保护策略和隐私保护技术手段的更新配置符合设计要求。	金融业务系统

8.10 监管支撑

8.10.1 交易信息监管

交易信息监管的评估内容见表120。

表120 交易信息监管评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应保证监管部门对用户身份能够进行审查和披露	1.查阅材料 2.查看系统	1.设计文档中明确用户需要提供真实的身份信息（如身份证号、护照号）进行注册后方可使用该系统。 2.系统注册时要求用户提供真实的身份信息。 3.系统中使用的密码机制和设计文档中一致，并且可以根据用户真实的身份信息生成匿名的用户身份标识，能够从匿名的身份信息中还原出用户的身份信息。	金融业务系统、科技产品
2	应保证监管部门对交易信息进行审查和披露	1.查阅材料 2.查看系统	1.开发文档中明确系统具有访问底层数据、提取交易记录和追溯交易信息的接口。 2.系统中加密的交易记录，能够还原成可以解读的信息。 3.系统能够按需查询或者分析特定的业务数据。	金融业务系统
3	应为监管部门提供交易干预的技术方式	查阅材料	1.设计文档中说明该系统具备的交易干预机制，包括但不限于取消用户交易权限、限制用户交易、冻结用户账户等。 2.使用手册中说明交易干预机制的使用方式。	金融业务系统、科技产品

8.10.2 系统监管

系统监管的评估内容见表121。

表121 系统监管评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应提供节点的状态信息	查看系统	1.系统日志提供了节点的运行状态信息。 2.系统日志提供了节点上提交的交易信息，用以判断节点的状态。	金融业务系统

8.10.3 应急事件报警

应急事件报警的评估内容见表122。

表122 应急事件报警评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具有紧急事件主动报警的能力	1.查阅材料 2.查看系统	1.设计文档中说明系统具有报警功能，并且能够在紧急事件发生时向监管部门及时报送事件信息。紧急事件包括但不限于系统遭遇攻击、系统大规模宕机、链上交易信息出现非法内容、	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
			用户信息遭遇大规模泄露等。 2.系统功能模块中具有与设计文档一致的功能。	

8.10.4 智能合约监管

智能合约监管的评估内容见表123。

表123 智能合约监管评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	宜将监管要求与管理要求写入智能合约中强制执行	查阅材料	1.设计文档说明智能合约中写入了监管要求与管理要求，包括但不限于交易行为统计、交易行为干预、交易信息可还原、用户信息可溯源、紧急事件报警与处理等，并且能够保证与监管和管理相关的智能合约强制执行。 2.智能合约的编码中具有监管要求与管理要求的相关代码，并实现设计文档中的功能。 3.智能合约的编码、注释、开发文档及其他与编码相关的文档中，智能合约具有合理性与合规性，不存在潜在的非法违规操作漏洞。	金融业务系统、科技产品

8.11 安全运维

8.11.1 权限管理

权限管理的评估内容见表124。

表124 权限管理评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应对敏感信息、重要数据和设备的访问权限、使用权限进行要求和限制	1.查阅材料 2.查看系统 3.访谈人员	1.设计文档中明确关于敏感信息、重要数据的访问相关接口调用进行权限限制。 2.系统配置文件中有访问控制列表。 3.管理文档中明确设立安全保密管理员，并由安全保密管理员严格限制敏感信息、重要数据和设备的访问权限和使用权限。 4.管理文档中明确设立安全审计员，并由安全审计员定期检查相关的接口是否存在非授权的调用、对相关接口的调用是否进行权限限制、是否成功阻止非授权的访问和使用敏感信息、重要数据和设备。	金融业务系统、科技产品

8.11.2 审计记录

审计记录的评估内容见表125。

表125 审计记录评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具有系统中关键事件的审计记录，并对审计记录进行相应的保护	查看系统	1.系统日志中具有关键事件产生审计记录，且至少包括：节点的版本升级与漏洞修复、系统中相关的重大安全事件、节点的加入与退出、重要设备和硬件的访问、使用等，且审计记录留存不少于6个月。 2.配置文件或审计相关的策略配置中能够明确负责生成与保存审计记录的节点。 3.系统的访问控制策略中明确限制不同等级的节点对于审计记录的访问与操作权限，能够防止审计记录被非法篡改或删除。	金融业务系统
2	应具有针对关键数据访问与使用的审计记录，并对审计记录进行相应的保护	1.查阅材料 2.查看系统	1.系统日志中具有针对关键数据访问与使用的审计记录，且审计记录留存不少于6个月。 2.管理制度中的说明审计记录的保存方式、策略，并明确负责管理与保存审计记录的责任部门或机构。 3.系统的访问控制策略中明确限制不同等级的用户、程序或接口对于审计记录的访问与操作权限，能够防止审计记录被非法篡改或删除。	金融业务系统、科技产品

8.11.3 系统更新

系统更新的评估内容见表126。

表126 系统更新评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备在不影响系统业务处理的情况下对节点的版本进行及时更新的能力	1.查阅材料 2.查看系统 3.访谈人员	1.主要节点的版本为业务系统必需的最新版本，且最新节点的版本能够向下兼容较旧版本的数据。 2.主要节点的升级策略能够避免大多数节点集中进行版本升级，升级策略能够保证系统业务保持正常可用。 3.管理员在测试环境中进行模拟版本升级后方可在正式环境中进行版本升级，具有在测试环境中充分验证版本升级的测试工具和文档。 4.应急预案中具有版本升级失败的应急方案，以保证节点在升级失败时能够在规定时间内恢复可用性。	金融业务系统

序号	实现要求	评估方法	结果判定	适用对象
			5.系统日志中留有节点版本升级的审计记录，保证节点的版本更新可追溯。	

8.11.4 漏洞修复

漏洞修复的评估内容见表127。

表127 漏洞修复评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备漏洞发现和漏洞修复的机制	1.查阅材料 2.查看系统 3.访谈人员	1.漏洞扫描策略涵盖节点服务器自身漏洞、软件漏洞、智能合约漏洞等不同层次的漏洞，扫描的周期至少每月一次。 2.漏洞扫描记录与漏洞扫描策略一致。 3.管理员对发现的安全漏洞能够及时的提出修复方案并申请修复审批，对于不能修复的安全漏洞，能够评估影响并及时报告。 4.管理员在测试环境中进行模拟漏洞修复后方可在真实环境中进行漏洞修复，并且漏洞修复后不会对节点的账本数据、密钥等关键业务数据产生影响。 5.系统日志中留有漏洞修复留有审批记录、审计日志，保证漏洞修复可追溯。	金融业务系统、科技产品

8.11.5 备份与恢复

备份恢复的评估内容见表128。

表128 备份恢复评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备关键数据的备份与恢复机制	1.查阅材料 2.查看系统	1.账本数据备份策略根据业务需要进行实时备份。 2.密钥等关键数据备份策略根据业务需要进行定期备份。 3.网络拓扑配置中明确备份数据采取异地备份的方式。 4.根据账本数据、密钥等关键数据的恢复策略定期进行恢复演练，最近一次的恢复演练记录表明备份数据的可用性，保证在出现重大事件时能够及时的进行数据恢复。	金融业务系统

8.11.6 应急预案

应急预案的评估内容见表 129。

表129 应急预案评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具有统一的应急预案框架，并制定重要事件的应急预案	查阅材料	1.应急预案框架中包括但不限于应急处理流程、应急组织构成、应急资源保障、事后教育和培训等内容。 2.针对重要事件的应急预案中包括但不限于应急处理流程、系统恢复流程等内容，重要事件包括但不限于节点账本数据损坏、针对系统出现大规模的攻击、系统因故障或升级失败等原因出现大规模宕机、交易回滚、链上交易信息出现非法内容、用户信息遭遇大规模泄露等。	金融业务系统

8.12 安全治理

8.12.1 系统安全管理机制

系统安全管理机制的评估内容见表 130。

表130 系统安全管理机制评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具备合理有效的系统安全管理机制	1.查阅材料 2.访谈人员	1.管理文档中明确系统安全管理机制至少包含日常管理团队和应急管理团队；日常管理团队至少包含传统安全管理人员如系统管理员、网络管理员、安全管理员等，还应包含金融业务风险管理人员以及安全管理员；应急管理团队具备在应急事件发生时进行必要的应急处置的能力。 2.具备实现安全治理所需的资质与能力。	金融业务系统、科技产品
2	系统安全管理机制应满足系统安全治理的要求	1.查阅材料 2.访谈人员	1.管理员使用网络管理工具、系统监控工具、系统运维工具等运维管理相关工具与各类系统故障处理方法说明文档、各类运维工具使用说明书等文档支撑实现运维管理的职责。 2.管理制度中具有用于实现安全治理目标的激励或制约等相关规章制度。	金融业务系统、科技产品

8.12.2 节点管理

节点管理的评估内容见表 131。

表131 节点管理评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	应具有确保系统安全运行所需的成员节点管理机制	1.查阅材料 2.查看系统 3.访谈人员	1.管理文档中明确新加入节点需实施准入控制，包括但不限于对节点真实身份的审查、对其他节点运行和记账的影响分析以及节点协议签署等，并说明相应审核流程。 2.设计文档中明确了新接入的节点需进行信息登记，并说明了信息验证的方式；新节点接入的登记信息中记录了节点基本软硬件信息、节点与机构的对应关系等信息。 3.设计文档中明确系统中具有节点退出的审议控制功能，具备参与节点“自愿退出”和“投票剔除”等不同的退出方式；用户手册中说明了节点退出相关功能模块的使用方式。 4.管理员进行节点管理操作前需要先进行身份验证，确保节点管理操作的合法授权。 5.系统日志中保留有完整的操作日志确保节点管理操作的可审计和可追溯。	金融业务系统、科技产品
2	应满足共识节点高可靠、高可用的安全管理要求	1.查阅材料 2.查看系统	1.设计文档中明确系统采用不同种类的节点实现版本，以保证系统整体稳定性的节点异构性，包括“部署异构”、“硬件异构”和“软件异构”；系统中网络拓扑配置、节点的版本、硬件型号与设计文档中一致。 2.设计文档中具有可靠节点数量低于共识节点要求的最低安全数量的预警与防范机制，并且设计文档中具有相关的功能模块的设计。 3.应急预案中具有可靠节点数量低于共识节点要求的最低安全数量的应急方案、处置措施。	金融业务系统、科技产品

8.12.3 干预机制

干预机制的评估内容见表132。

表132 干预机制评估内容表

序号	实现要求	评估方法	结果判定	适用对象
1	宜从用户、节点、系统的不同层面进行有效干预	查阅材料	1.设计文档中明确系统具有禁止或限制单个用户系统操作的功能，并在用户手册中说明该功能模块的使用方法。 2.设计文档中明确系统具有临时终止或应急强制终止节点的功能，并在用户手册中说明该功能模块的使用方法。	金融业务系统、科技产品

序号	实现要求	评估方法	结果判定	适用对象
			3.设计文档中明确系统具有大规模节点关断或系统关断等实施系统干预的功能，在用户手册中说明该功能模块的使用方法，并且在应急预案中明确系统干预后的恢复策略、恢复方案和具体措施。	
2	宜具备合理的干预权限管理和干预行为管理	1.查阅材料 2.查看系统 3.访谈人员	1.管理员在使用干预功能前需要进行身份验证。 2.访问控制策略中明确具备干预权限的管理账户，并且将干预权限分散给多个指定用户，避免系统账户由于包括指定对象的账户而受到影响并且防范分布式病毒攻击所带来的风险。 3.系统日志中记录了干预行为的操作历史，并将操作记录存储在系统中与所有节点进行共识，确保操作历史不可更改并且可以被查询，做到可审计、可追溯。	金融业务系统、科技产品