中 国 区 块 链 测 评 联 盟 标 准

CBTCA-001-2019

区块链与分布式记账信息系统评估规范

Grading Evaluation Specification for Blockchain and Distributed Ledger Information System

2019 - 1 - 9 发布　　2019 - 1 - 9 实施

中国区块链测评联盟　发 布

目　　次

前　言

在当前科技重大变革的时代，区块链作为集合了技术、模式、机制等多维度价值的技术独树一帜，成为瞩目的热点。作为一种新兴的应用模式，其发展是需要时间和过程的，没有捷径可走，只能脚踏实地服务实体经济，才能体现出技术的价值。然而，技术本身正处于探索阶段，产品研发、应用推广、标准研制、测试评价等工作理应同步推进。区块链的标准化有助于统一对区块链的认识，辨识区块链的真伪，规范和指导高质量的区块链在各行业的发展，促进区块链的共性技术攻关，对于促进区块链产业健康发展意义重大。

为积极响应国家号召，推动中国区块链技术、应用和产业健康有序发展，争夺国际区块链发展话语权，为国家网络强国战略和构建人类命运共同体建设贡献力量，助推中国区块链产业发展和支撑体系建设，全面保障高质量国家主权区块链基础平台建设。中国区块链测评联盟组织成员单位开展区块链相关标准研制工作。标准研制的流程和标准参考国际标准和行业标准研制的相关规则和规定，标准工作组聚集了国内区块链行业多个领域的技术和管理专家，开展了多种形式的专题研讨、专家和企业征求意见活动，在保证标准专业性的同时，也确保了标准研制过程的公开性和透明性。

本标准负责起草单位：工业和信息化部电子第五研究所、北京蓝石环球区块链科技有限公司、北京航空航天大学、北京邮电大学、火币中国、无锡井通网络科技有限公司、北京云测信息技术有限公司、北京版全家科技发展有限公司、青岛墨一客区块链有限公司、北京软件和信息服务交易所有限公司、北京中百信信息技术股份有限公司、烨链(上海)科技有限公司、北京科技大学、浙江数秦科技有限公司、布比（北京）网络技术有限公司、安妮股份、新能区块链有限公司、上海圳链网络科技有限公司、成都链安科技有限公司、安徽井畅数字技术有限公司、清华x-lab区块链3.0研究院、简约互动科技（北京）有限公司、北京大禹通证科技有限公司、东港股份有限公司、远光软件股份有限公司、成都三泰智能科技有限公司、四川国科链科技有限公司等。

本标准主要起草人：相里朋、刘赫、宾建伟、李劭辉、高传富、郭莉、周沙、袁煜明、类承叁、郝汉、王毛路、张筱、卢学哲、蒋晓军、胡骏、朱岩、钟宏、杨霞、于铁强、徐欧、朱立、彭仁夔、艾洋、蔡维佳、黄晏清、张谦、苗知秋、田朝晖、田家昌、罗伟宸、翟伟伟、邓肯、杨胜、李军、曲勋杰、刘钢锋、胡智威、刘庆波、刘泰金、周海平、郝佳诺、杨杰、宣宏量、孙绍祥、刘宏、明月明、董虹等。

使用帮助信息：任何单位和个人在使用本标准的过程中，若存在疑问，或有对本标准的改进建议和意见，请与中国区块链测评联盟联系。

电话：18611861869；电子邮件：dh@bluecefa.com

通信地址：蓝石科技北京公司（北京市朝阳区柳芳北里6号楼西侧）

引　言

未来已来，区块链如约而至。从互联网建立信息互联以来，我们建立起信息的互联关系，基于此实现了人人互联，未来更是会实现万物互联。而当信息、人、物互联完成后，价值互联必将成为现实，其核心要素便是信任，在低成本情况下运行的信任。

区块链技术有望解决“三元悖论”，其通过分布式方式来建立可信的机制，将从传统的人和人之间的模式，转化为对机器的信任；价值转移渠道从高成本的中介通道，转变为基于区块链的低成本安全通道；社会治理模式从传统的信息技术辅助模式，转化为基于规则的法治模式，帮助建立行业基础可信环境，实现个人和机构的商业、社会信用数据的跨行业融合。

从市场平台来讲，区块链正逐步成为一种市场的工具，帮助社会来削减平台的成本，让中间机构成为过去，促使公司现有业务模式重心的转移，加速公司发展；从底层技术来讲，区块链正加速数据记录、数据传播和数据存储管理模式的转型；从社会结构来看，区块链正推动法律与经济融为一体，颠覆原有社会的监管和治理模式。

本标准从区块链的标准化出发，制定区块链系统评测相关标准，统一对区块链的认识，规范和指导区块链在各行业的发展，促进解决区块链的关键技术问题，有助于加强我国国家主权区块链基础平台的研发，对于区块链产业生态发展意义重大。

刘　赫　　博士
蓝石区块链实验室 主任
二零一九年一月

区块链与分布式记账信息系统评估规范

1 范围

本部分规定了区块链与分布式记账信息系统（简称“区块链信息系统”）的技术要素、质量模型，提出了定量评估和定性评估的评估内容和方法。

本部分适用于：

——甲方建设区块链信息系统，指导区块链技术和产品选型，开展系统评估工作；

——乙方开展区块链产品和技术服务，研发区块链信息系统，选择技术要素和业务功能。

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。

CBD-Forum-001-2017 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。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

[CBD-Forum-001-2017 区块链 参考架构]

3.2 分布式记账技术 Distributed Ledger Technology

一种以分布式的方式共享和同步的账本技术。

[ISO/AWI 23257 Blockchain and Distributed Ledger Technologies--Reference Architecture]

3.3 零知识证明 Zero Knowledge Proof

一种证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的算法。

3.4 群签名 Group Signature

一种群体中任意一个成员可以匿名的方式代表整个群体对消息进行签名的技术

3.5 环签名 Ring Signature

一种简化的群签名技术，环签名中只有环成员没有管理者，不需要环成员间的合作。

3.6 盲签名 Blind Signature

一种接收者在不让签名者获取所签署消息具体内容的情况下所采取的一种特殊的数字签名技术。

3.7 可替代性通证 Fungible Token

一种满足以太坊ERC-20通证标准要求，可互相替代的通证。

3.8 不可替代性通证 Non-Fungible Token

一种满足以太坊ERC-721通证标准要求，唯一且不可替代的通证。

4 系统质量

4.1 技术参考要素

4.1.1 技术参考架构

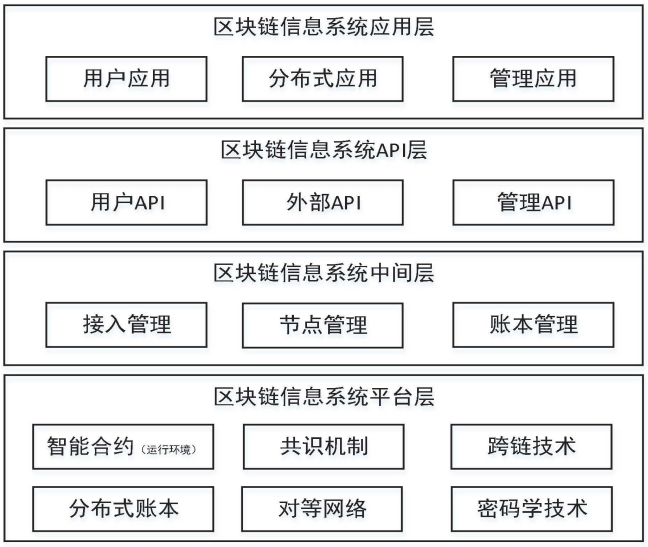

图1 技术参考架构

本技术参考架构（图1），参考ISO/AWI 23257 《Blockchain and Distributed Ledger Technologies—Reference Architecture》，分为区块链信息系统平台层、中间层、API层、应用层等。

4.1.2 平台层要素

平台层需提供区块链信息系统正常运行的运行环境和基础组件，包括分布式账本、对等网络、密码学技术、共识机制、跨链技术和智能合约（运行环境）等。

4.1.2.1 分布式账本

4.1.2.1.1 分布式存储

分布式存储应提供账本运行中各类数据的存储能力，分布式存储应支持：

a) 账户、事务、交易等数据正确写入、使用和查询；
b) 高效、稳定、安全的数据服务。

4.1.2.1.2 节点运算

节点运算应提供账本稳定运行的算力支持，节点运算应支持：

c) 支持区块链信息系统运行环境；
d) 支持数值、符号等计算，且计算能力满足节点运行要求。

4.1.2.1.3 时序服务

时序服务应提供账本运行中的行为、数据和记录一致性的时序支持，时序服务应支持：

a) 支持统一账本记录时序内容；
b) 支持时序容错性内容；
c) 支持集成可信第三方时序服务内容。

4.1.2.1.4 账本记录

账本记录应提供一种通过不同节点对账本的共同记录与维护，形成区块链信息系统中数据的公共管理、防篡改、可信任的机制，用于支持中间层的账本管理组件，账本记录应支持：

a) 支持持久化的账本记录存储；
b) 支持一次或多次查询或记录请求的结果一致；
c) 支持账本的多个节点拥有完整相同的事务记录、区块记录等；
d) 支持确保节点账本记录相同的数据一致性；
e) 支持区块链大小的动态或静态调整；
f) 支持完整账本或局部账本的同步，支持对账本选择性同步；
g) 支持全量账本或局部账本的快速检索。

4.1.2.2 对等网络

对等网络应提供采用P2P通信协议实现的数据和信息交换，用于支持中间层的节点管理组件，对等网络应支持：

a) 支持基于软硬件保障的安全通信机制；
b) 支持基于广播或多播协议的通信播存能力；
c) 支持节点静态或动态的加入、退出机制；
d) 支持网络抖动时的自动恢复、自我管理等自适应机制；
e) 支持节点状态和信息动态更新与获取；
f) 支持节点类型、能力等配置信息的参数化。

4.1.2.3 密码学技术

4.1.2.3.1 加解密

加解密应提供一种或多种满足用户安全需求的加密算法、模块、服务或设备，实现数据的安全加解密能力，加解密应支持：

a) 支持国际 AES256 或国内 SM4、SM7 等对称加密算法；
b) 支持国际 RSA、ECC 或国内 SM2、SM9 等非对称加密算法；
c) 支持可插拔、易替换的加解密算法模块；
d) 支持基于硬体实现的安全加解密设备；
e) 支持基于硬件实现的密钥管理接口。

4.1.2.3.2 数字摘要

数字摘要应提供一种或多种满足用户安全需求的哈希散列算法，实现数据的摘要值（Hash值）求解，保障数据的完整性，数字摘要应支持：

a) 支持国际 SHA256 或国内 SM3 等哈希散列算法；
b) 支持自定义高计算复杂性的数字摘要算法；
c) 支持基于硬体实现的哈希散列求解设备。

4.1.2.3.3 数字签名验签

数字签名验签应提供一种或多种满足用户安全需求的数字签名/验签算法，实现对事务的签名和验签，保障数据完整性和不可伪造性，数字签名验签应支持：

a） 支持国际 RSA、ECC 或国内 SM2、SM9 等数字签名/验签算法；
b） 支持可插拔、可替换的数字签名/验签算法模块；
c） 支持基于硬体实现的数字签名/验签设备。

4.1.2.3.4 CA 认证

CA认证应提供一种或多种满足用户安全需求的CA认证机制，实现可信的网络身份认证，保障数据单元的完整性和不可伪造性，CA认证应支持：

a） 支持私有证书或国密证书的网络身份认证；
b） 支持私有 CA 提供的客户端、服务节点 CA 认证；
c） 支持第三方 CA 提供的客户端、服务节点 CA 认证。

4.1.2.3.5 隐私保护

隐私保护应提供一种或多种满足用户安全需求的隐私保护方式机制，实现身份、交易等的保护，隐私保护应支持：

a） 支持采用公钥地址或脱敏数据代表交易身份信息的全匿名或部分匿名的身份隐私保护；
b） 支持采用交易哈希或脱敏数据代表交易详情的全匿名或部分匿名的交易隐私保护；
c） 支持监管、审计或特殊账户在授权下，明文查看身份及交易信息；
d） 支持客户端私钥的隐私保护，需通过身份认证确认有权使用，且使用过程不以明文读取、传输或存储；
e） 支持服务节点私钥的隐私保护，需通过身份认证确认有权使用，且使用过程不以明文读取、传输或存储。

4.1.2.4 共识机制

共识机制应提供一种或多种节点间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，共识机制应支持：

a) 支持 PoW、POS、DPoS、PBFT、DAG 等一种或多种共识算法；
b) 支持可插拔替换的混合共识机制；
c) 支持满足场景需求的节点数、与交易共识及结果确认；
d) 支持节点独立对共识过程的事务进行有效性验证；
e) 支持多节点通过共识机制实现容错。

4.1.2.5 智能合约

智能合约（运行环境）应提供一种或多种智能合约的开发、调试、运行环境，保障合约安全可信运行，智能合约（运行环境）应支持：

a) 支持 C/C++、Java、JS、Golang 等一种或多种编程语言；
b) 支持 Vmware、Docker 等虚拟技术的集成开发、调试及运行环境；
c) 支持合约运行的正确性，合约运行在各节点的结果正确且一致；
d) 支持合约运行的可终止性，合约运行可在合理范围、有限时间内结束；
e) 支持合约运行的可交互性，合约运行可与外部数据源间进行交互；
f) 支持合约的可审计性，提供合约部署、发布、运行的审计接口；
g) 支持合约的防篡改性，应防止合约在未授权下篡改达成共识的内容。

4.1.2.6 跨链技术

跨链技术应提供区块链信息系统间进行资产、数据互操作的技术，跨链技术应支持：

a) 支持两两互联、网络路由、代理商等一种或多种跨链方式；
b) 支持跨链交易的原子操作，跨链交易结果应保持一致；
c) 支持链间的资产互换，资产未实质性转移，仅拥有者发生变更；
d) 支持链间的资产转移，资产实质性转移，拥有者也发生变更；
e) 支持跨链重构（分叉）风险控制，防止重构导致链间资产总数变化。

4.1.3 中间层要素

中间层需提供区块链信息系统调用平台层的基本功能，并为API层提供接入管理接口，包括接入管理、节点管理、账本管理等。

4.1.3.1 接入管理

接入管理应提供平台层进程调用能力，为API层提供账户体系、区块、事务等接入管理接口，接入管理应支持：

a) 支持账户体系相关的信息查询和配置管理服务；
b) 支持区块、事务、通证的信息查询和配置管理服务；
c) 支持接口访问权限的信息查询和配置管理服务；
d) 支持多链管理的信息查询和配置管理服务。

4.1.3.2 节点管理

节点管理应提供节点的管理控制能力，为API层提供节点状态、网络状态、参数化配置等节点管理接口，节点管理应支持：

a) 支持节点服务器的节点状态的信息查询和配置管理服务；

b) 支持节点及节点服务的启动与关闭控制管理服务；
c) 支持节点服务能力的参数化配置服务；
d) 支持节点服务器网络连接状态监控服务；
e) 支持节点事务处理、账本查询等授权配置服务；
f) 支持 RPC、WebSocket、REST-API 等调用模式，启动或关闭节点管控服务；
g) 支持节点热升级管理和配置服务。

4.1.3.3 账本管理

账本管理应提供账本记录的管理控制能力，为API层提供签名权限设置、记录逻辑验证等账本管理接口，账本管理应支持：

a) 支持链上内容的发行、新增、分配和交换服务；
b) 支持账本记录的逻辑验证、结果验算服务；
c) 支持账本记录的签名权限设置服务。

4.1.4 API 层要素

API层需调用中间层功能组件为用户应用、管理应用和分布式应用提供可靠和高效访问的功能，并提供统一的访问和节点管理，包括用户API、管理API和外部API等。

4.1.4.1 用户 API

用户API应提供一个可对用户业务功能进行访问的应用程序编程接口，用户API应支持：

a) 支持接口调用中间层的相关组件，访问平台层相关数据；
b) 支持接口提供用户应用微服务，支撑应用层对接使用；
c) 支持链上用户权限和数据的配置能力。

4.1.4.2 管理 API

管理API应提供一个可对系统管理功能进行访问的应用程序编程接口，管理API应支持：

a) 支持接口调用中间层的相关组件，访问平台层相关数据；
b) 支持接口提供管理应用微服务，支撑应用层对接使用；
c) 支持链上管理权限和数据的配置能力。

4.1.4.3 外部 API

外部API应提供一个可对外部数据源或函数进行访问的应用程序编程接口，外部API应支持：

a) 支持接口调用中间层的相关组件，访问平台层相关数据；
b) 支持接口提供分布式应用微服务，支撑应用层对接使用；
c) 支持外部可信数据源或函数访问能力。

4.1.5 应用层要素

应用层需将不同类型的API封装成业务相关功能，提供区块链信息系统的访问和使用，包括用户应用、管理应用和分布式应用等。

4.1.5.1 用户应用

用户应用应提供客户访问和使用区块链的功能，用户应用应支持：

a) 支持命令行交互方式访问和使用区块链；

b) 支持图形化交互方式访问和使用区块链；
c) 支持音视频交互方式访问和使用区块链；
d) 支持第三方应用程序访问和使用区块链。

4.1.5.2 管理应用

管理应用应提供管理者访问和使用区块链的功能，管理应用应支持：
a) 支持区块链成员管理相关功能，提供身份管理、权限管理等；
b) 支持区块链事务管理相关功能，提供预定义事务管理、自定义事务管理等；
c) 支持区块链安全管理相关功能，提供状态查询、安全服务等；
d) 支持区块链监控管理相关功能，提供故障监测、网络状态监控、运行状态监控等；
e) 支持区块链配置管理相关功能，提供参数配置、告警配置、安全配置等；
f) 支持区块链日志管理相关功能。

4.1.5.3 分布式应用

分布式应用应由智能合约提供的区块链业务功能，分布式应用应支持：
a) 支持区块链服务的选择订购和退订；
b) 支持区块链状态信息的查询和使用；
c) 支持事务提交状态的查询和使用；
d) 支持数据上链和应用上链，满足业务处理和应用要求。

4.2 质量参考模型

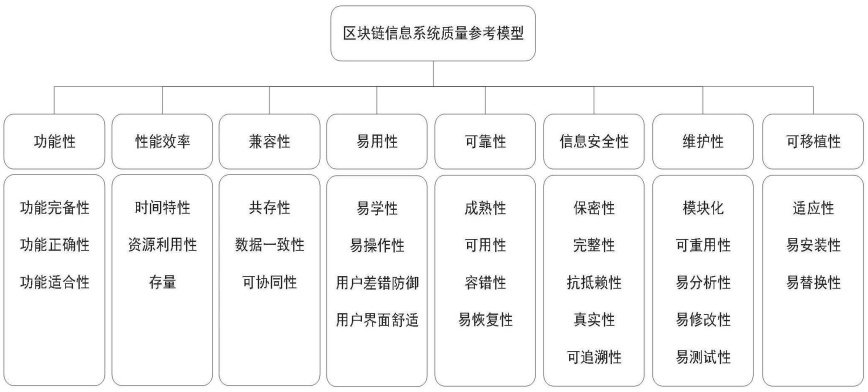

图 2 质量参考模型

本质量参考模型（图2），依据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》，分为功能性、性能效率、兼容性、易用性、可靠性、信息安全性、维护性、可移植性等。

4.2.1 功能性

功能性指区块链信息系统具备完成相应处理或流程能力的程度。

a) 功能完备性指系统在相关功能范围内，无需额外借助或添加其他元素来实现相应业务能力的完全性程度；
b) 功能正确性指对所有可能的测试输入，系统能按预期结果运行，即满足规定的业务规格说明并完成业务功能目标的程度；
c) 功能适合性指系统满足实际需求的特性，即场景运行与实现过程中完成指定的任务和目标实现的程度。

4.2.2 性能效率

性能效率指区块链信息系统对于各类性能的体现结果。
a) 时间特性指通过在系统上运行规定的业务负载时在响应时间、处理时间及吞吐率方面符合需求的程度；
b) 资源利用性指通过在系统上运行规定的业务负载时，消耗资源的数量和类型符合需求限制的程度；
c) 存量指系统的最大极限符合负载的程度。

4.2.3 兼容性

兼容性指区块链信息系统在共享相同的硬件或软件环境的条件下，可正常运行且与其他产品、系统或组件交换信息的程度。
a) 共存性指系统与其他产品共享同一云服务环境和资源条件下，能够有效执行所需功能且不会对其他产品造成负面影响的程度；
b) 数据一致性指系统实现降低数据同步延迟，保证数据的一致性，避免造成数据混乱和失准的程度；
c) 可协同性指系统实现与其他系统间的互操作的程度。

4.2.4 易用性

易用性指区块链信息系统在有效性、效率和满意度特性方面，可满足指定的用户使用的程度。
a) 易学性指在用户学习使用系统的方便的程度；
b) 易操作性指系统具有易于操作和控制的属性的程度；
c) 用户差错防御指系统预防用户犯错的程度；
d) 用户界面舒适指系统的界面提供令人愉悦和满意的交互的程度。

4.2.5 可靠性

可靠性指区块链信息系统在指定条件下、指定时间内执行指定功能的程度。
a) 成熟性指在一个时间周期内运行规定的业务时，系统的可靠运行程度；
b) 可用性指在一个时间周期内运行规定的业务时，系统的可访问程度；
c) 容错性指在出现故障或违反规定接口的情况下，系统维持规定性能级别的能力；
d) 易恢复性指功能发生中断或失效的情况下，系统恢复受损数据并重建正常状态的能力。

4.2.6 信息安全性

信息安全性指区块链信息系统保护信息和数据的程度，及用户、产品或系统具有与其授权类型和授权级别一致的数据访问度。
a) 保密性指系统确保其数据只能被授权用户访问的能力程度；
b) 完整性指系统防止未授权访问、篡改程序或数据能力程度；

c） 抗抵赖性指系统针对活动或事件发生后可以被证实且不可被否认的能力程度；
d） 真实性指系统对目标或资源的身份标识确实能够证实该目标或资源的能力程度；
e） 可追溯性指系统可唯一追溯到特定使用者相关活动的能力程度。

4.2.7 维护性

维护性指区块链信息系统被特定人员有效修改和维护的程度。
a） 模块化指在维护过程中，系统功能模块对实施维护的支持程度；
b） 可重用性指模块或模块代码可用于其他软件或系统的程度；
c） 易分析性指诊断缺陷或失效原因易被分析的程度；
d） 易修改性指模块或模块代码易实施修改的程度；
e） 易测试性指已修改组件易被确认的程度。

4.2.8 可移植性

可移植性指区块链信息系统可从一种硬件、软件或其他运行（使用）环境迁移到另一种环境的有效性和效率的程度。
a） 适应性指在使不同的约束条件下系统正常运行的程度；
b） 易安装性指系统文件在特定环境中能有效部署的程度；
c） 易替换性指在相同软件、硬件环境下，替换同类产品的难易程度。

5 评估要求

区块链信息系统的评估过程，应采用专业测评手段和工具，对区块链信息系统的技术特性及系统功能性、性能效率、信息安全性等开展评估。

5.1 评估内容

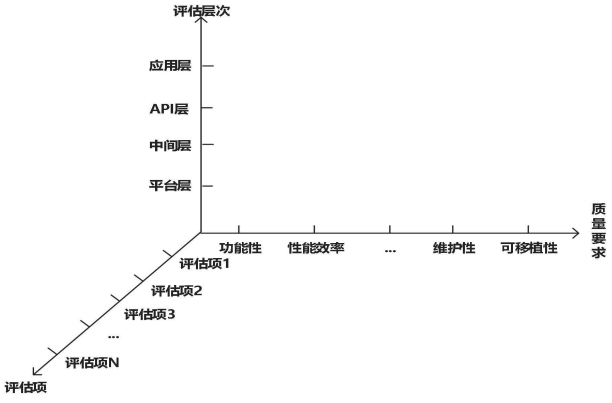

图 3 区块链信息系统评估内容

本评估（图3）包括定性评估和定量评估两类，评估时应根据“附录B”选定评估内容，结合上述评估层次和质量要求对区块链信息系统开展具体评估工作。

a) 评估层次参考技术参考要素，分为区块链信息系统平台层、中间层、API层、应用层等；

b) 质量要求参考质量参考模型，分为功能性、性能效率、兼容性、易用性、可靠性、信息安全性、维护性、可移植性等。

5.2 评估方法

5.2.1 定性评估

应用下述评估策略（表1）对选定的评估项开展定性评估工作，并对评估结果给出“是否通过”的结论。

表 1 定性评估

评估结果	划分标准	是否通过	分值
严重不符合	存在不能执行正常功能或重要功能，或者危及人身安全严重缺陷，或严重不符合性能、安全等要求	否	0
一般不符合	存在影响系统要求或基本功能的实现，或不符合性能、安全等要求，但存在合理的解决办法	否	0.3
存在改进项	不存在主要功能失效、性能改进、严重安全等问题，存在一些建议整改内容	是	0.6
满足要求	评估子项测试通过，符合性能、安全和功能等要求	是	1

注：评估结果的分值将作为定量评估时，计算评估项得分X_{ij}（$X_{ij} \in [0,1]$）的输入项。

5.2.2 定量评估

根据“附录A”对所有定性评估结果进行评估计算，给出定量评估数值。并应用下述评估策略（表2），将定量评估结果划分为基础级、增强级三级、增强级二级和增强级一级等。

表 2 定量评估

要素	基础级	增强级三级	增强级二级	增强级一级
评估结果	$X \in [60,70)$	$X \in [70,80)$	$X \in [80,90)$	$X \in [90,100]$

推荐适用领域，如表3所示。

表 3 推荐适用领域

要素	适用领域

基础级	推荐适用于一般企业、集团公司、事业单位等非核心场景
增强级三级	推荐适用于地市级国家机关、重要企事业单位等核心场景
增强级二级	推荐适用于跨省、市联网运行的用于生产、调度、管理、作业、指挥等关键场景
增强级一级	推荐适用于重要领域、重要部门的铁路、民航、电力、核心、军工等关键场景

附 录 A
（规范性附录）
评估计算方法

区块链信息系统评估计算方法如表A.1所示。首先依据自身需求，分配测评子要素权重（推荐权重供参考）；其次依据评估方法给出个子要素得分；最终依据评估计算方法，计算出评估总分。

$$X = \frac{\sum_{i=1}^{n} X_i}{n} \times 100 \qquad (i=1,2,3,...n) \quad (1)$$

$$X_i = \sum_{j=1}^{n} (W_{ij} * X_{ij}) \qquad (j=1,2,3,...n) \quad (2)$$

式中：
X——为系统测评总得分，$X \in [0,100]$；
X_i——为评估层次得分，$X_i \in [0,1]$；
X_{ij}——为评估项得分，$X_{ij} \in [0,1]$；

W_{ij}——为评估项权重，$W_{ij} \in [0,1]$，$\sum_{j=1}^{n} W_{i,j} = 1$, $i=1,2,3,...n$

表 A.1 评估项计算表

评估层次	评估层次得分	评估项	评估项权重	评估项得分
平台层	X_1	分布式账本	22.66%	X_{11}

		对等网络	15.63%	X_{12}
		密码学应用	13.28%	X_{13}
		共识机制	19.53%	X_{14}
		智能合约（运行环境）	18.75%	X_{15}
		跨链技术	10.16%	X_{16}
中间层	X_2	接入管理	35.42%	X_{21}
		节点管理	31.25%	X_{22}
		账本管理	33.33%	X_{23}
API 层	X_3	用户API	22.92%	X_{31}
		管理 API	22.92%	X_{32}
		外部 API	22.92%	X_{33}
应用层	X_4	用户应用	31.25%	X_{41}
		管理应用	31.25%	X_{42}
		分布式应用	37.50%	X_{43}
评估总分	X			

表A.2用于计算每个评估子项所占的权重（推荐权重供参考），子项重要性越高、其权重越大，标红的评估子项需重点关注。

表 A.2 评估子项计算表

评估子项		分布式账本	对等网络	密码学应用	共识机制	智能合约（运行环境）	跨链技术	接入管理	节点管理	账本管理	用户API	管理API	外部API	用户应用	管理应用	分布式应用	总权重
功能性	功能完备性	10%	10%	4%	10%	10%	4%	10%	10%	4%	4%	4%	4%	4%	4%	4%	100%
	功能正确性	7%	7%	7%	7%	7%	7%	7%	7%	7%	7%	7%	7%	7%	7%	7%	100%
	功能适当性	10%	5%	10%	10%	10%	5%	5%	10%	5%	5%	5%	5%	5%	5%	5%	100%
性能效率	时间特性	20%	20%	0	20%	10%	0	0	0	0	10%	10%	10%	0	0	0	100%
	资源利用率	30%	30%	0	30%	10%	0	0	0	0	0	0	0	0	0	0	100%

	存量	100%	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100%
兼容性	共存性	0	0	0	35%	35%	0	5%	5%	5%	0	0	0	5%	5%	5%	100%
	数据一致性	18%	18%	0	18%	18%	0	0	0	0	9%	9%	9%	0	0	0	100%
	可协同性	20%	0	20%	20%	20%	20%	0	0	0	0	0	0	0	0	0	100%
易用性	易学性	14%	14%	0%	14%	14%	0%	7%	7%	7%	0	0	0	7%	7%	7%	100%
	易操作性	14%	14%	0%	14%	14%	0%	7%	7%	7%	0	0	0	7%	7%	7%	100%
	用户差错防御	13%	0%	13%	13%	13%	13%	6%	6%	6%	0	0	0	6%	6%	6%	100%
	用户界面舒适	14%	14%	0%	14%	14%	0%	7%	7%	7%	0	0	0	7%	7%	7%	100%
可靠性	成熟性	13%	13%	25%	25%	13%	13%	0	0	0	0	0	0	0	0	0	100%
	可用性	11%	6%	11%	11%	6%	6%	6%	6%	6%	6%	6%	6%	6%	6%	6%	100%
	容错性	17%	8%	0	17%	8%	8%	17%	0	0	8%	8%	8%	0	0	0	100%
	易恢复性	50%	50%	0	0	0	0	0	0	0	0	0	0	0	0	0	100%
信息安全性	保密性	11%	0	22%	0	0	0	0	22%	0	11%	11%	11%	0	0	11%	100%
	完整性	17%	0	17%	17%	0	0	0	0	17%	8%	8%	8%	0	0	8%	130%
	抗抵赖性	8%	0	15%	15%	15%	0	0	0	15%	8%	8%	8%	0	0	8%	100%
	可追溯性	10%	0	20%	20%	0	0	20%	0	0	10%	10%	10%	0	0	0	100%
	真实性	14%	14%	14%	0	0	0	14%	7%	14%	0	0	0	7%	7%	7%	100%
维护性	模块化	8%	8%	8%	8%	8%	8%	8%	8%	8%	0	0	0	8%	8%	8%	100%
	可重用性	8%	8%	8%	8%	8%	8%	8%	8%	8%	0	0	0	8%	8%	8%	100%
	易分析性	8%	8%	8%	8%	8%	8%	8%	8%	8%	0	0	0	8%	8%	8%	100%
	易修改性	8%	8%	8%	8%	8%	8%	8%	8%	8%	0	0	0	8%	8%	8%	100%
	易测试性	8%	8%	8%	8%	8%	8%	8%	8%	8%	0	0	0	8%	8%	8%	100%
可移植性	适应性	0	0	0	29%	29%	0	0	0	0	0	0	0	14%	14%	14%	100%
	易安装性	50%	0	0	50%	0	0	0	0	0	0	0	0	0	0	0	100%
	易替换性	14%	0	0	29%	29%	0	29%	0	0	0	0	0	0	0	0	100%

附 录 B
（规范性附录）
评估项一览表

表 B.1 平台层评估子项一览表

评估层次 / 质量要求	评估项		评估子项
功能性	分布式账本	分布式存储	1)对等网络中，能够被每个节点部署并使用，对等网络能够被每个节点查询[*]。 2)每条数据记录过程使用共识性来验证，并能追溯到唯一审计线索或业务规则。
		节点运算	1)对等网络中，计算能力能够满足每个节点要求[*]； 2)提供可视化监控，以便评价系统弹性和数据完整性； 3)支持通过容器、状态机、微服务等类似技术，加速提升计算能力。
		时序服务	1)支持统一账本记录时序（时间戳）等内容[*]。 2)具备时序容错性、容错共识算法等内容； 3)支持集成可信第三方硬件时序服务等内容。
		账本记录	1)支持持久化存储账本记录，包括技术库种类、数据库指标、账本存储格式、区块格式规范等内容[*]； 2)多个节点拥有完整账本的记录，支持完整账本同步； 3)系统确保有相同账本记录的各节点的数据一致性； 4)支持关系型数据库、非关系型数据库，且数据库指标（安全性、兼容性、可扩展性）符合用户需求； 5)支持账本信息，交易信息存入关系型数据库，且账本存储格式、区块格式规范等内容符合用户需求； 6)支持账号信息和账本中支持的数据结构存入非关系型数据库，且账本存储格式、区块格式规范等内容符合用户需求； 7)链上与非链上的数据记录可拥有完整账本的记录； 8)链上与非链上的数据记录支持数据回退检查步； 9)支持账本隐私保护，未经权限许可无法查看与之无关的隐私内容。 10)支持区块链大小的动态或静态调整； 11)支持节点间通过账本同步，保证各节点间数据一致； 12)支持完整账本或局部账本的同步，对账本选择性下载； 13)支持全量账本或局部账本的快速检索； 14)支持一次或多次查询或记录请求具有相同结果。

评估层次 质量要求	评估项		评估子项
功能性	对等网络		1)支持点对点之间的安全通信[*]； 2)提供点对点通信基础上的多播能力； 4)支持节点即插即用，即对节点新增和退出的动态； 5)支持 zabbix 类似技术，监控节点状态和多服务节点，支持对节点的信息和状态及时获得； 6)支持对节点的参数化配置，对节点类型和能力进行设定； 7)支持 protobuf 类似协议，压缩通信数据； 8)支持从时空两相上考察网络结构； 9)支持网络结构满足空间上的一致性； 10)支持网络结构满足网络演化过程性质演变。
	密码学应用	加解密	1)支持国际主流加密算法，如 AES256 等对称加密算法和 RSA、ECC 等非对称加密算法[*]； 2)支持我国商密算法，如 SM4、SM7 等对称加密算法和 SM2、SM9 等非对称加密算法； 3)支持可插拔、易替换的加解密算法模块； 4)支持基于硬件实现的安全加解密设备； 5)支持可插拔自定义的密码算法； 6)支持基于硬件实现的密钥管理接口； 7)支持具有隐私保护机制的密钥管理接口； 8)支持全流程基于国密算法完成加解密操作； 9)支持前沿加解密算法，如同态加密、动态加解密等。
		数字摘要	1)支持国际 SHA256 或国内 SM3 等哈希散列算法[*]； 2)支持自定义高计算复杂性的数字摘要算法； 3)支持能够抗量子攻击的数字摘要算法； 4)支持基于硬体加速的哈希散列求解设备； 5)基于摘要算法构造的内容索引结构具备模糊搜索功能； 6)基于摘要算法构造的内容索引结构满足安全性要求。
		数字签名	1)支持国际主流的数字签名算法，如 RSA、ECC 等[*]； 2)支持通过本地签名，保证用户秘钥安全； 3)支持我国商密的数字签名算法，如 SM2 等； 4)支持自定义高计算复杂性的算法； 5)支持国密算法生成的 CA 证书； 6)数字签名算法能够抵抗量子攻击； 7)数字签名算法具备消息恢复功能； 8)数字签名算法具备权益委托功能； 9)数字签名算法的安全性满足用户要求。
		CA 认证	1)支持基于密钥的身份验证，防止身份冒用； 2)支持基于第三方 CA 机构完成客户端的 CA 认证； 3)支持基于第三方 CA 机构完成服务节点的 CA 认证； 4)支持国家授权的第三方 CA 机构签发的国密证书。

评估层次 质量要求	评估项		评估子项
功能性		隐私保护	1)支持全匿名或部分匿名的隐私保护，即不公开交易双方的身份详细信息，可使用公钥地址表示交易双方身份； 2)支持全匿名或部分匿名的隐私保护，即不公开交易双方的交易细节，对交易信息进行加密以实现隐私保护； 3)对审计或超级权限账户保持交易透明，对非监管账户保持隐私保护； 4)客户端私钥只允许其所有者读取，存储和传输需有保护措施，不能以明文方式传输或存储，且客户端进出需经过身份验证； 5)服务节点私钥只允许其所有者读取，存储和传输需有保护措施，不能以明文方式传输或存储，且节点进出需经过身份验证； 6)支持前沿隐私保护算法，如零知识证明、环签名、盲签名、群签名等； 7)节点信息具备分层保护功能。
	共识机制		1)支持多个节点参与共识和结果确认[*]； 2)支持独立节点对信息的正确性进行验证； 3)支持一定的共识机制容错性； 4)支持节点广播哈希区块到其他节点； 5)支持在区块链上进行事务的验证查询的过程； 6)物理故障情况下，节点不丢失数据； 7)满足共识机制条件少数节点无法恶意篡改账本数据。
	智能合约（运行环境）		1)提供编程语言支持(Go、Lua、JavaScript 等)的集成开发环境，合约源代码或二进制查询； 2)提供 Vmware、Docker 类似虚拟运行载体支持； 3)支持合约同步或异步调用方式，调用结束即会返回结果； 4)支持依据合约复杂度进行收费方式，以保护复杂合约运行； 5)支持智能合约代码和逻辑的静态、动态检查功能； 6)支持智能合约部署前注册、发布前审计功能； 7)支持与外部数据源交互，且影响范围仅限本合约； 8)防止恶意对合约内容进行篡改； 9)智能合约的编写满足特定安全性需求； 10)支持多方共识下的合约内容升级，合约具备完整的生命周期管理； 11)支持向账本中写入合约内容，注册合约和部署合约的复杂程度。
	跨链技术		1)支持跨链交易的原子化，即交易要么发生，要么不发生，不存在任何中间状态； 2)支持跨链交易确认，即确认跨链交易在原链确实有发生且已被原链节点最终确认； 3)支持两两互联、跨链平台或类似网络路由，实现多条链之间的跨链。 4)支持重构（分叉）风险控制，重构可能会导致两条链的资产总数发生变化，从而导致跨链交易失效； 5)跨链不能影响或降低原有链的安全性； 6)跨链节点支持一种或多种公证人、侧链、中继链等机制； 7)跨链节点支持一种或多种 HTLC、哈希锁定等技术。

评估层次 / 质量要求	评估项	评估子项
性能效率	资源利用性	1)考察传输带宽负载满足度，即执行规定的数据传输功能时，所占用的最大传输带宽符合需求的限制； 2)数字摘要算法的性能满足用户要求； 3)基于摘要算法构造的内容索引结构满足性能要求.； 4)数字签名算法的性能满足用户要求。

注：“*”指标代表“终止项”，若该指标未通过评估，则评估结果不合格。

表B.2 中间层评估子项一览表

评估层次 质量要求	评估项	评估子项
功能性	接入管理	1)对账户体系相关信息提供基本查询服务； 2)对账户体系相关的业务提供服务； 3)将客户提交的特定事务操作请求提交到区块链网络； 4)对区块总高度、指定高度的查询服务； 5)对事务的查询服务； 6)对特定事务进行相关操作的功能； 7)对接口调用频度进行管理功能； 8)对接口查询进行缓存的功能； 9)对接口访问方式进行相关配置的功能； 10)对账户体系相关的业务提供的服务功能。
	节点管理	1)提供区块链节点服务器的节点状态信息查询服务； 2)提供区块链节点服务器的启动与关闭服务； 3)提供区块链节点服务器的节点服务能力配置； 4)提供区块链节点服务器网络连接状态监控服务； 5)对节点服务的启动和关闭功能进行管控； 6)对节点的启动和关闭功能进行管控； 7)对节点参与的共识算法进行相关配置； 8)对节点的提供服务能力和最大负载进行配置； 9)对节点间的网络状态、连接数量和资源消耗进行监控； 10)对节点加入网络的准入/准出权限进行配置； 11)节点进行事务处理时结果满足预期要求的能力； 12)节点以外的节点事务记录是否测试节点一致； 13)节点支持多因子认证机制； 14)节点支持细粒度访问控制； 15)节点支持使用物理令牌。

评估层次 质量要求	评估项	评估子项
	账本管理	1)对链上内容发布、交换； 2)对共识前的逻辑验证和共识后的结果验算； 3)对特定事务处理进行多签名权限控制设置； 4)通过配置来对账本查询权限进行控制； 5)通过相关配置来对账本禁止查询权限进行控制； 6)共识前对特定标识的资产进行逻辑验证； 7)共识前对资产数额进行逻辑验证； 8)共识后对共识结果的验证； 9)通过多个签名来对权限进行控制； 10)采用特定事务的多重签名进行控制和验签操作； 11)通过多个签名来对事务进行验证； 12)通过智能合约组件来执行智能合约代码； 13)支持特定事务的批量操作； 14)支持用户大数据上链操作。

表B.3 API层评估子项一览表

评估层次 质量要求	评估项	评估子项
功能性	用户 API	1)支持用户 API 调用中间层的相关组件，访问平台层相关数据； 2)支持用户 API 提供用户应用微服务，支撑应用层对接使用； 3)支持链上用户权限和数据的配置能力； 4)支持通过 WSS 协议保证用户 API 与底层通信安全； 5)支持上层应用和用户 API 通过 HTTPS 保证通信安全。
	管理 API	1)支持管理 API 调用中间层的相关组件，访问平台层相关数据； 2)支持管理 API 提供管理应用微服务，支撑应用层对接使用。 3)支持链上管理权限和数据的配置能力； 4)支持通过 WSS 协议保证管理 API 与底层通信安全； 5)支持上层应用和管理 API 通过 HTTPS 保证通信安全。
	外部 API	1)支持外部 API 调用中间层的相关组件，访问平台层相关数据； 2)支持外部 API 提供分布式应用微服务，支撑应用层对接使用； 3)支持外部可信数据源或函数访问能力； 4)支持通过 WSS 协议保证外部 API 与底层通信安全； 5)支持上层应用和外部 API 通过 HTTPS 保证通信安全。
性能效率	资源利用率	1)测量 I/O 设备占用率，即指定 I/O 设备在每个单位时间内，设备繁忙时间所占的比例。

表B.4 应用层评估子项一览表

评估层次 / 质量要求	评估项		评估子项
功能性	用户应用		1)命令行功能实现交互； 2)图形化界面实现交互； 3)系统图形的已有功能交互完全； 4)系统应用程序的已有功能交互完全； 5)系统事务提交的已有功能交互完全。
	分布式应用		1)可对区块链服务进行自主选择或取消； 2)可对区块链服务进行订购和退订； 3)可调用账本辅助业务操作； 4)业务功能是否能够满足用户需求。
	管理应用	成员管理服务	1)对成员的身份进行管理； 2)对成员的权限进行相关管理； 3)对成员的数据隐私安全进行的管理； 4)对成员的身份、行为等进行的追溯审计。
		监控管理	1)提供区块链信息系统故障监测； 2)提供区块链网络运行状态的监控服务。
		其他管理	1)提供区块链服务客户账号安全性的服务； 2)提供预定义或自定义事件的服务，包括预定义事件功能、自定义事件功能等； 3)提供区块链网络问题跟踪、报告的服务，包括网络问题跟踪及报告等。
性能效率	资源利用性		1)考察 CPU 占用率满足度，即处理器执行非闲置线程时间的最大百分比符合需求的限制； 2)考察内存占用率满足度，即用于运行进程有效物理内存的平均数量符合需求的限制； 3)考察外存时间负载满足，即运行效率测试过程中，外存被独占的时间的符合需求的限制； 4)考察外存空间占用率满足度，即已使用外存空间符合需求的限制。
	时间特性		1)考察响应时间满足度，即任务命令的响应时间长度满足需求； 2)考察周转时间满足度，即作业开始到作业完成所需的时间间隔满足需求； 3)考察吞吐率满足度，即单位时间处理的任务数量满足需求。
	存量		1)考虑最大请求数满足度，即在要求的负载下，单位时间内可处理最大请求数量满足需求； 2)考察事务累积容量满足度，即在要求的负载下，可处理的最大累积事务数量满足需求； 3)考察数据吞吐容量满足度，即在规定的时间内，可处理完成最大数据量达满足需求； 4)考察数据处理容量满足度，即对于指定的数据处理或数据存储功能，可处理的最大数据量满足需求。
兼容性	数据一致性		1)考察系统运行规定的业务，数据同步延迟及数据一致性程度。
	可协同性		1)考察与其他区块链进行数据协同程度； 2)考察不同链间互操作，遵循通信协议、统一 API、区块数据格式的协同程度。
易用性	易学性		1 考察)在有效性、效率、抗风险和满意度特性方面用户学习使用的难度。
	易操作性		1)考察系统具有易于操作和控制的属性的程度。
	用户差错防御		1)考察系统预防用户犯错的程度。

评估层次 质量要求	评估项	评估子项
	用户界面舒适	1)考察系统的界面提供令人愉悦和满意的交互的程度。
可靠性	成熟性	1)考察实际完成的验证任务与需完成的验证任务之比； 2)考察已纠正的缺陷与已发现缺陷之比满足要求的程度； 3)考察一定运行周期内的软件发生故障间隔时间的平均值满足要求的程度； 4)考察在确定的测量单位的软件中发现的故障数量满足要求的程度； 5)考察在确定的测量单位的软件中发现的缺陷数量满足要求的程度； 6)考察系统中最大容忍节点失败个数； 7)考察系统中最大容忍节点欺骗个数； 8)考察网络抖动对于系统服务等级的影响情况。
	可用性	1)考察系统实际提供的服务时间与需提供的服务时间之比； 2)考察在特殊条件下，系统正常运行的时间； 3)考察一定运行周期内的系统无法提供服务的平均时间； 4)考察节点的容纳能力是否满足用户需求。
	容错性	1)考察系统隔离风险的能力，如在硬件设计错误或软件设计缺陷时，节点仍能正常工作； 2)考察未导致宕机的失效与系统失效之比； 3)考察未引起失效的系统故障与已发现故障之比； 4)考察系统实际实现的抵御误操作的有效设计在应设计的抵御误操作中的占比； 5)考察常见黑客网络攻击的抵御能力，如抵抗拒绝服务攻击、侧信道攻击等。 6)考察异构环境下的数据通信容错能力。
	易恢复性	1)考察在异常事件或在需要时，系统复原到失效前或指定状态的能力； 2)考察有效备份数据在需备份数据中的占比； 3)考察在宕机后，系统能在要求的时间内成功重新启动与重新启动次数之比； 4)考察故障发生时，系统通告故障花费的时间。
信息安全性	保密性	1)考察未授权的访问区块链数据时，数据隐私情况是否满足要求； 2)考察系统对未授权的访问操作进行控制的能力是否符合需求； 3)考察系统对未授权的数据访问进行控制的能力是否符合需求； 4)考察系统对数据项实现加密/解密的比例是否符合需求； 5)考察系统对数据项进行正确的加密/解密的能力是否符合需求； 6)考察已被审核通过的加密算法所占的比例。
	完整性	1)考察系统防止数据被讹误能力是否符合需求； 2)考察系统防止数据被讹误所采取的方法是否符合需求。
	抗抵赖性	1)考察数据采用数字签名传输是否符合需求； 2)考察系统防止实体否认发送事件及其行为的能力； 3)考察系统防止实体否认接收事件及其行为的能力。
	真实性	1)考察系统使用的身份鉴别方法是否符合需求； 2)考察系统在安全数据上实现的鉴别规则数量是否符合需求。

评估层次 质量要求	评估项	评估子项
	可追溯性	1)考察日志进行安全保存的实际时间是否符合需求； 2)考察用户访问系统和数据进行审计追踪的能力是否符合需求； 3)考察用户记录的访问类型进行审计追踪的能力是否符合需求。
维护性	模块化	1)考察模块结构符合需要，包括代码、预定义的代码的程度； 2)考察模块间存在的依赖关系的强弱。
	可重用性	1)考察系统模块能用于其他系统的程度； 2)考察代码的注释遵从注释规范的程度； 3)考察代码的编写遵从代码编写规范的程度； 4)考察文档的编写遵从文档编写规范的程度。
	易分析性	1)考察系统准确的诊断维护点的程度； 2)考察系统诊断维护目标所需的时间满足用户期待的时间的程度； 3)考察系统提供充分的维护线索以支持维护实施的程度； 4)考察系统维护过程提供的线索易理解的程度； 5)考察当系统发生缺陷、失效或需要修改时能有效的追踪的程度。
	易修改性	1)考察维护指定的功能是否易通过修改代码完成； 2)考察软件变更、修订的版本是否易被标识； 3)考察配置参数是否易变更，来实施修改； 4)考察变更周期，用户问题是否能在可接受的时间内解决； 5)考察维护过程是否相对容易，通过执行得以解决问题； 6)考察系统是否具有撤销等类似功能，在完成修改后，可正常还原到修改前状态。
	易测试性	1)考察在维护后，是否易使用测试用例再次执行测试； 2)考察测试工作是否易通过搭建自动验证流程完成。
可移植性	适应性	1)考察系统对于支撑软件变化的适应能力； 2)考察系统易被用户掌握的能力； 3)考察系统对于硬件环境变化的适应能力； 4)考察系统对于操作系统、数据库变化的适应能力； 5)考察系统对于通信环境、数据结构变化的适应能力。
	易安装性	1)考察在移植过程中，系统部署包安装到新环境后是否正常运行； 2)考察在移植过程中，系统的部署包安装和卸载的难易程度； 3)考察在移植过程中，网络搭建的复杂程度。
	易替换性	1)考察软件更新，升级或替换其他软件后，相同的数据是否可继续使用； 2)考察功能内含性，系统更新，升级或替换其他系统后，类似功能是否可正常使用； 3)考察升级或替换其他系统后，新功能与用户期望的一致，是否能被用户接受； 4)考察遵照移植标准和架构等容器的设计对接的程度。

附 录 C
（规范性附录）
评估项打分表

评估层次 / 质量要求	平台层	中间层	API层	应用层
功能性	*12*	*5*	*8*	*13*
性能效率	…	…	…	…
兼容性				
易用性				
可靠性				
信息安全性				
维护性				
可移植性				

注：根据表A.1和表A.2，对评估层次、质量要求等维度的区块链信息系统的评估项进行打分。

参 考 文 献

[1] 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

[2] CBD-Forum-001-2017 区块链 参考架构

[3] 贵阳市人民政府新闻办公室. 贵阳区块链发展和应用白皮书，2017.

[4] 中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书，2018.

[5] ISO/AWI 23257 Blockchain and Distributed Ledger Technologies—Reference Architecture, 2018.

[5] The Ethereum Foundation. Ethereum Homestead Documentaion, http://www.ethdocs.org/en/latest. 2018.

[6] The Ethereum Foundation. ERC-20 Token Standard, https://eips.ethereum.org/EIPS/eip-20. 2018.

[7] The Ethereum Foundation. ERC-721 Token Standard, https://eips.ethereum.org/EIPS/eip-721. 2018.