许可链测评指南（V1.1）

中国区块链生态联盟

青岛市崂山区人民政府

2018年6月

前 言

区块链（Blockchain）是分布式存储、共识机制、点对点通讯、加密算法等计算机技术在互联网时代的集成式创新，具有安全、防篡改、可证信、高度可扩展等特点，正成为继大数据、云计算、人工智能、虚拟现实等技术后又一大将对未来产生重大影响的新兴技术，有望推动人类从信息互联网时代步入价值互联网时代。

区块链来源于比特币等加密数字货币，并且实现了大规模应用，但其应用价值已远远超出了加密数字货币的范畴。区块链的技术特征非常适合在不信任或弱信任的环境下建立信任关系，重塑组织架构，降低中介成本，规范商业秩序，目前正在向数字资产鉴权、供应链管理、物联网、智能制造、物流管理、金融科技等领域快速延伸，具有很好的应用前景。

伴随着区块链的诞生，对其质量风险质疑和讨论始终没有停止，区块链的安全问题、性能问题等被热议。尽管比特币、以太坊等知名加密数字货币在互联网基本稳定的运行了多年，但公有链平台与基于许可链的行业应用在访问控制、加密算法、共识机制、节点管理等方面并不完全一致，如何客观合理的验证区块链产品的质量成为学术界和产业界共同面临的问题。

在山东省青岛市崂山区政府的大力支持下，中国区块链生态联盟委托赛迪（青岛）区块链研究院和中国软件评测中心组织专家力量，编撰形成了《许可链测评指南（V1.0）》。指南的核心内容是许可链的测评指标及方法，以期对许可链产品研发单位、应用单位及第三方技术服务单位等提供关于许可链质量验证的参考，也作为中国区块链生态联盟开展许可链测评认证的重要技术依据。

本指南基于赛迪（青岛）区块链研究院和中国软件评测中心技术人员对许可链的技术理解和多年的测评工作经验编写而成，并经过了中国区块链生态联盟内专家和领导的评审，但由于能力和水平所限，疏漏和不足之处在所难免，敬请广大读者和专家批评指正。区块链的技术在不断进步，应用领域在不断拓展，我们也将不定期的更新指南内容。

**编写单位**(排名不分先后)

赛迪（青岛）区块链研究院

中国软件评测中心

**主要编写人员**（排名不分先后）

刘 权、刘法旺、曾 晋、黄忠义、袁 方、王 喆、吕 韬、万晨阳、刘曦子

**主要技术顾问**（排名不分先后）

# 背景介绍

## 区块链概述

区块链（Blockchain）起源于化名为中本聪（Satoshi Nakamoto）的技术极客或团体在2008年发表的文章《比特币：一种点对点电子现金系统》，本质上，区块链是比特币及大量加密数字货币的底层实现技术体系，但加密数字货币仅是区块链的一种应用场景，时至今日区块链的价值已远远超出了加密数字货币范畴。当前，我国的一些研究机构、互联网企业等均高度关注区块链的发展，部分企业发布了区块链白皮书、技术产品和解决方案，同时一些新生的区块链企业和研究机构也围绕着区块链的技术创新、产品服务和产业生态做了大量的工作。

从技术角度来说，区块链是分布式存储、共识机制、点对点通讯、加密算法等技术的集成式创新。在典型区块链系统中，数据以区块（block）为单位产生和存储，每个区块中记录了一个时间段内按照某种算法挑选打包的交易，且区块按照出块顺序连成链式（chain）数据结构。新创建的区块通常需得到全网多数（具体数量决于不同的共识机制）节点的确认，并向各节点广播实现全网同步，之后不能更改或删除，实现交易记录的不可篡改和可追溯。区块链网络中的所有节点共同参与区块链系统的数据验证、存储和维护，以保证系统和数据的高可靠性。

目前来看，区块链的核心价值在于通过多种技术的融合，在不信任或弱信任环境下实现信息对称（即共享账本），进而重塑了信用体系和组织结构，有助于保障业务数据公开透明、可溯源、难以被非法篡改，在数字资产鉴权、物联网、智能制造、物流管理、供应链金融等领域有很好的应用前景。尽管区块链能够有助于构建信任机制、转变现有的商业模式，但是我们也要清醒的意识到，目前区块链在认知理解、技术实现、标准规范、商业模式等方面仍不尽完善，需要进行大量的探索和研究工作。

## 区块链分类

区块链系统根据应用场景和设计体系的不同，一般分为公有链、联盟链和私有链。其中：

——公有链的各个节点可以自由加入和退出网络，并参加链上数据的读写，运行时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点。

——联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。

——私有链的各个节点的写入权限收归内部控制，而读取权限可视需求有选择性地对外开放。私有链仍然具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。

许可链是指参与到区块链系统中的每个节点都是经过许可的，未经许可的节点是不可以接入到系统中，因此联盟连和私有链都属于许可链。

## 许可链测评

通过对目前产业及技术的分析，当前阶段基于区块链的行业应用以许可链为主（包括私有链和联盟链）。许可链作为区块链的一种应用模式，可以规避公有链安全风险、性能效率问题以及一些政策法规的限制。事实上，许可链乃至区块链的技术实际上仍处于发展阶段，因此我们基于对区块链的理解以及开展测评工作的经验，编写了《许可链测评指南》，旨在引导大众对许可链的认知、规范许可链产品的技术质量、明确许可链产品的评价体系。以本指南为基础，中国区块链生态联盟将委托赛迪（青岛）区块链研究院将和中国软件评测中心等单位开展许可链测评认证工作。

# 测评范围

本指南主要针对许可链产品的技术特性进行测评，主要包括许可链的数据操作、账户管理、共识机制、加密算法、智能合约、性能效率、节点管理、运维管理等8个领域的32个测评指标项，在具体的测试实施过程中，实施单位可以根据具体情况将每个测评指标项细化为不同的测评用例，这里我们暂时不做具体要求。

# 许可链测评指标及方法

## 数据操作

### 查询区块平均生成时间、总区块数

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品是否具备查询区块平均生成时间、总区块数的功能 |
| **测评步骤** | 1. 通过调用许可链产品SDK、智能合约及命令行指令，查询当前区块链上总区块数 2. 查看当前区块平均生成时间 |
| **预期结果** | 可查看当前许可链产品上总区块数和平均生成时间 |

### 查询指定区块业务数量

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品是否具备查询指定区块中业务数量的功能 |
| **测评步骤** | 1. 通过调用许可链产品SDK、智能合约及命令行指令，随机选择一个区块 2. 查看该区块中的业务数量 |
| **预期结果** | 可查看指定区块中的业务数量 |

### 查询指定区块业务明细

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品是否具备查询指定区块中业务明细的功能 |
| **测评步骤** | 1. 通过调用许可链产品SDK、智能合约及命令行指令，随机选择一个区块 2. 查看该区块中的业务明细 |
| **预期结果** | 可查看指定区块中的业务明细 |

### 点对点业务处理

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具有点对点业务处理的功能 |
| **测评步骤** | 1. 发起从一个账户向另一个账户的业务处理/状态变更请求 2. 对于交易类（如交易）等业务处理，测试最小单位是否支持，验证最大上限是否溢出；对于溯源、资产转移等状态变更，测试状态变更情况 |
| **预期结果** | 1. 若接受账号不存在，则报告错误 2. 交易类业务请求，系统转出和转入的价值总量（可考虑业务手续费）相同；状态变更类业务请求，对应账号的状态信息得到有效变更 |

### 业务溯源

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品是否具备指定业务溯源的功能 |
| **测评步骤** | 1. 通过调用许可链产品SDK、智能合约及命令行指令，针对某业务进行系统索引查询 2. 查看该区块中的业务历史明细 |
| **预期结果** | 可查看指定业务历史明细 |

## 账户管理

### 账户注册

|  |  |
| --- | --- |
| **测评目的** | 验证产品具有账号注册功能 |
| **测评步骤** | 1. 发起账户注册的申请，填写注册信息 2. 验证账户是否创建成功 3. 再次发起创建同一个账号的请求 |
| **预期结果** | 1. 创建成功，系统保存用户账户信息，并返回创建成功的信息 2. 不重复存储账号信息，并返回不能重复创建或创建失败的信息 |

### 账户信息修改

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具有用户账户信息修改的功能 |
| **测评步骤** | 1. 发起用户账户信息的修改 2. 查询用户账户信息 |
| **预期结果** | 1. 修改成功，系统更新用户账户信息，并返回成功 2. 查询账户信息为最新修改后的信息 |

### 账户冻结

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具有用户账户的注销功能 |
| **测评步骤** | 1. 发起冻结用户账户 2. 用已冻结的账户重新登录或直接发起一笔业务，验证是否停止使用 |
| **预期结果** | 冻结成功，已冻结的账户不能再进行登录或发起业务失败 |

### 账户权限控制

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品用户账户是否具有访问权限控制功能 |
| **测评步骤** | 1. 通过区块链权限控制功能对某账户进行访问权限设置，包括智能合约、SDK等接口的访问权限 2. 该账户通过命令行访问接口 3. 未赋予权限的账户通过命令行访问接口 |
| **预期结果** | 1. 具有权限的账户能够访问接口 2. 其他不具有权限的账户访问被拒绝 |

## 共识机制

### 无故障、无欺诈的共识

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品在无故障和无欺诈的情况下达成共识的能力 |
| **测评步骤** | 1. 发起一笔合法业务请求 2. 发起一笔非法业务请求 |
| **预期结果** | 1. 合法业务请求，共识成功 2. 非法业务请求，共识失败 |

### 双花攻击防范

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品在处理“双花攻击”的防范能力 |
| **测评步骤** | 发起一笔合法业务请求，对某个节点的接受请求消息进行“双  花”业务验证 |
| **预期结果** | 接受到被重放请求的节点拒绝“双花”的请求 |

### 容错能力

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品网络的共识机制是否支持节点容错 |
| **测评步骤** | 1. 确保许可链产品网络中节点数满足最少节点数要求，并在网络中随机设置宕机节点和恶意节点 2. 发起一笔合法业务的请求 3. 发起一笔非法业务的请求 |
| **预期结果** | 1. 合法业务请求，共识成功 2. 非法业务请求，共识失败 |

## 加密算法

### 链上内容的加密传输与存储

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品对链上私有信息通过加密传输与存储 |
| **测评步骤** | 1. 账户设置私有信息并进行加密 2. 若区块链产品支持多种加密算法（国密、商密），重复操作1，调用不同的加密算法加密 3. 查看业务是否被加密 |
| **预期结果** | 1. 信息密文存储 2. 信息密文传输 |

### 平台加密算法的支持

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品身份授权功能对加密算法的支持性 |
| **测评步骤** | 1. 通过许可链产品提供的接口，调用加密算法进行验证 2. 若区块链产品支持多种加密算法（国密、商密），重复操作1对不同的加密算法进行验证 3. 查看验证结果是否正确 |
| **预期结果** | 1. 身份授权密文存储 2. 身份授权密文传输 |

## 智能合约

### 智能合约执行结果

|  |  |
| --- | --- |
| **测评目的** | 通过实际执行智能合约，查看结果是否正确 |
| **测评步骤** | 1. 启动区块链节点 2. 构建、发起满足智能合约规则的交易 3. 触发对应智能合约 4. 查看执行结果是否与逻辑推理的结果一致 |
| **预期结果** | 构建测试智能合约，并触发执行，最后的执行结果是否与逻辑推理的结果一致 |

### 查询支持

|  |  |
| --- | --- |
| **测评目的** | 验证智能合约是否支持索引、区间、历史查询等功能 |
| **测评步骤** | 1. 编写智能合约并在区块链网络中部署调 2. 通过命令行执行该智能合约 |
| **预期结果** | 1. 系统返回此智能合约的所有查询的具有相同索引的信息 2. 系统返回此智能合约的所有查询区间信息 3. 系统返回此智能合约的所有查询历史信息 |

### 3.5.3智能合约更新

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具有智能合约动态更新的功能 |
| **测评步骤** | 1. 升级区块链系统智能合约，保原有智能合约作废 2. 查看运行结果 |
| **预期结果** | 升级完成后自动执行新版本智能合约，且系统稳定运行 |

### 3.5.4合约冻结或终止

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具有冻结/终止智能合约的功能 |
| **测评步骤** | 1. 对智能合约执行冻结/终止操作 2. 发起业务，运行智能合约，提示合约已冻结或终止，且无法正常执行 |
| **预期结果** | 合约冻结/终止后无法正常运行 |

### 3.5.5智能合约移植

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品是否支持智能合约移植 |
| **测评步骤** | 1. 升级区块链产品，并将老版本区块链上的智能合约移植到新版本区块链上 2. 运行智能合约 |
| **预期结果** | 区块链产品升级后，智能合约可移植到新版本区块链上且能正常运行 |

## 性能效率

### TPS（Transaction Per Second）

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品的业务请求的TPS |
| **测评步骤** | 1. 设置性能测试工具压力参数 2. 区块链链接配置、区块链节点数参数、区块链统计参数 3. 运行命令，启动压力 4. 基于区块大小（推荐指标：1MB）进行测试 5. 基于网络节点（推荐指标：4 个）进行测试 6. 基于模拟业务发生量TPS 进行测试 7. 查询测试结果 |
| **预期结果** | 可以查询到TPS |

### 节点故障恢复效率

|  |  |
| --- | --- |
| **测评目的** | 测量许可链产品网络节点的账本补齐时间 |
| **测评步骤** | 1. 将一个网络节点暂停一段时间后恢复 2. 测量该节点账本恢复到可记账状态所需时间 |
| **预期结果** | 1. 恢复的节点可以继续正常运行 2. 可以得出账本恢复时间与暂停时间之间的关系 |

### 交易确认时延

|  |  |
| --- | --- |
| **测评目的** | 测量许可链产品网络的最长和平均交易时延 |
| **测评步骤** | 1. 使用同一账号，在同一节点，以均匀的速率发起交易（时长应为出块时间的6倍） 2. 记录下每笔交易的确认时延，计算最长以及平均交易时延 3. 使用不同账号，在不同节点，以均匀的速率发起交易（时长应为出块时间的6倍） 4. 记录下每笔交易的确认时延，计算最长以及平均交易时延 |
| **预期结果** | 1. 可以计算出使用同一账号，在同一节点的最长以及平均交易时延 2. 可以计算出使用不同账号，在不同节点的最长以及平均交易时延 |

### 扩展性

|  |  |
| --- | --- |
| **测评目的** | 测量许可链产品节点的扩展性 |
| **测评步骤** | 1. 在正常运行的区块链产品中至少增加与当前节点数相同的节点 2. 观察产品的TPS 3. 观察产品的故障恢复能力 4. 观察产品的交易确认时延 5. 持续观察24小时 |
| **预期结果** | 产品的吞吐量、故障恢复能力及确认时延没有较大波动 |

## 节点管理

### 新增节点

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具有在不停机的情况下新增节点的功能 |
| **测评步骤** | 1. 系统正常运行，新节点部署后，发起新增节点的请求，校验新增节点的许可证明 2. 发起业务，验证新增节点可以正常工作，共识 |
| **预期结果** | 系统正常运行，新增节点加入到集群中，并能与集群中的节点进行共识，本地账本进行对应同步 |

### 删除节点

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具有在不停机的情况下删除节点的功能 |
| **测评步骤** | 1. 对已加入集群的节点进行删除节点的操作 2. 查看系统配置检查报告(系统硬件，服务环境，区块链等信息) 3. 发起一笔业务，测试删除节点是否还能进行共识 |
| **预期结果** | 系统正常运行，删除节点不能进行共识 |

### 节点账本同步

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品新增节点可自动同步网络账本 |
| **测评步骤** | 1. 新增一个节点，发起新增节点的请求 2. 节点加入网络后查看账本是否自动同步账本 |
| **预期结果** | 新加入节点可自动同步网络账本 |

### 区块配置修改

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品可灵活修改区块的配置 |
| **测评步骤** | 1. 配置区块的生成时间 2. 修改共享账本的容量限制 |
| **预期结果** | 基于新的区块生成时间和区块大小系统正常运转，并达成全网新的共识 |

### 节点访问权限授权

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品各个节点是否具有账本访问权限控制功能 |
| **测评步骤** | 1. 通过区块链权限控制功能对某节点进行访问权限设置，包括授权访问或同步区块链账本功能 2. 该节点通过命令行访问已授权账本 3. 该节点通过命令行访问未授权账本 4. 在稳定运行的区块链网络中新增一个节点并通过命令行访问账本 5. 对新增节点重复上述操作1至操作3 |
| **预期结果** | 1. 具有权限的节点能够访问账本 2. 其他不具有权限的接口访问被拒绝 3. 不具有权限的新增节点访问被拒绝 4. 具有权限的新增节点能够访问授权账本 |

### 节点访问接口权限授权

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品各个节点是否具有接口访问权限控制功能 |
| **测评步骤** | 1. 通过区块链权限控制功能对某节点进行接口访问权限设置，包括智能合约、SDK等接口的访问权限 2. 该节点通过命令行访问接口 3. 未赋予权限的节点通过命令行访问接口 4. 在稳定运行的区块链网络中新增一个节点通过命令行访问接口 5. 对新增节点重复操作1至操作3 |
| **预期结果** | 1. 具有权限的节点能够访问接口 2. 其他不具有权限的接口访问被拒绝 3. 不具有权限的新增节点访问被拒绝 4. 具有权限的新增节点能够访问接口 |

## 运维管理

### 新增节点的稳定性

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具备在新增节点下确保应用层业务稳定可用的能力 |
| **测评步骤** | 1. 请求应用层服务 2. 新节点部署后，发起新增节点的请求 3. 在新增节点过程中，持续请求应用层服务 4. 持续观察24小时 |
| **预期结果** | 1. 应用层服务可用 2. 新增节点加入到集群中，并能与集群中的节点进行共识 3. 在新增节点过程中，应用层服务可用 |

### 删除节点的稳定性

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具备在删除节点下确保应用层业务可用的能力 |
| **测评步骤** | 1. 请求应用层服务 2. 已加入集群的节点进行删除节点的操作 3. 在删除节点过程中，持续请求应用层服务 4. 持续观察24小时 |
| **预期结果** | 1. 应用层服务可用 2. 被删节点被移除出集群，并无法与集群中的节点进行共识 3. 在删除节点过程中，应用层服务可用 |

### 修改节点配置的稳定性

|  |  |
| --- | --- |
| **测评目的** | 验证许可链产品具备在修改节点配置下确保应用层业务可用的能力 |
| **测评步骤** | 1. 请求应用层服务 2. 对已加入集群的节点进行修改节点配置的操作 3. 在修改节点配置后，持续请求应用层服务 4. 持续观察24小时 |
| **预期结果** | 1. 应用层服务可用 2. 修改节点配置成功，继续能与集群中的节点进行共识 3. 在修改节点配置的过程中，应用层服务可用 |

# 许可链评价

按照测评流程，在许可链测评结束后应对被测产品进行评价，具体的评价准则一般由测评机构依据相关标准规范制定，同时还应综合考虑许可链产品的应用场景及所承载的业务类型。在此我们不具体论述，只是给出一些参考建议。

（1）一票否决制

顾名思义，该方案要求必须所有的指标均通过测评才能整体的给出“通过”的评价结果，只要有一项指标不通过测评，则整体上给予“不通过”的评价。

（2）加权评估法

根据实际的业务场景，实施测评的单位可以给予每个指标相同的分值，该项指标测评通过即可得到该分值，不通过则得0分，同时根据不同指标项的重要性赋予不同的权重系数，最终加权求和即可得到该被测产品的总得分，根据总得分情况给予“通过”或“不通过”的评价。

（3）综合加权评估法

在加权评估的基础上，对于一些重点特性的指标，建议采用一票否决制。例如如果某许可链产品无法实现业务溯源功能或无法新增节点，显然该许可链平台不具备实际运行的能力，不仅该指标项是“不通过”的评价，而且建议这样的被测产品整体上给予“不通过”的评价。