ICS 35.020
L 70

DB61

陕 西 省 地 方 标 准

DB 61/T 1283—2019

区块链安全测评 指标体系

Blockchain Security Assessment—Indicator system

2019－11－27 发布　　2019－12－27 实施

陕西省市场监督管理局　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由陕西省工业和信息化厅提出并归口。

本标准起草单位：西安电子科技大学、西安西电链融科技有限公司、陕西省网络与信息安全测评中心、广东安创信息科技开发有限公司。

本标准主要起草人：刘景伟、裴庆祺、李志奇、杨帆、赵首花、陈晨、杨向东、何果、梁天宇、李晓璐。

本标准由西安电子科技大学负责解释。

本标准首次发布。

联系信息如下：

单位：西安电子科技大学

电话：15802971220

地址：西安市太白南路2号

邮编：710071

区块链安全测评 指标体系

1 范围

本标准规定了区块链系统的安全架构、测评模型、测评指标体系和测评技术要求。

本标准适用于区块链安全系统的测试评价。

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 25069 信息安全技术 术语

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

在网络环境下，通过透明、可信的规则，构建的不可伪造、不可篡改和可追溯的分布式数据库。

3.2

共识算法 consensus algorithm

在分布式的网络环境下，使区块链各节点间达成一致的计算方法。

3.3

分布式账本 distributed ledger

在多个站点、不同地理位置或者多个机构组成的网络里实现共同治理及分享的资产数据库。

3.4

智能合约 smart contract

基于预定事件触发、不可篡改、自动执行的计算机程序。

4 区块链安全测评指标体系

4.1 评测模型

区块链安全测评模型如图1所示。

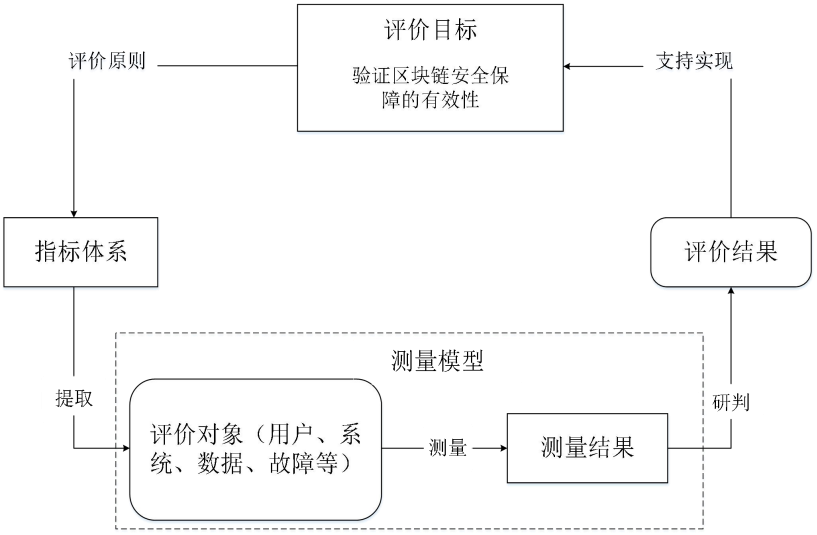

图 1　区块链安全测评模型

4.2　测评指标体系

区块链安全测评指标体系如图2所示。

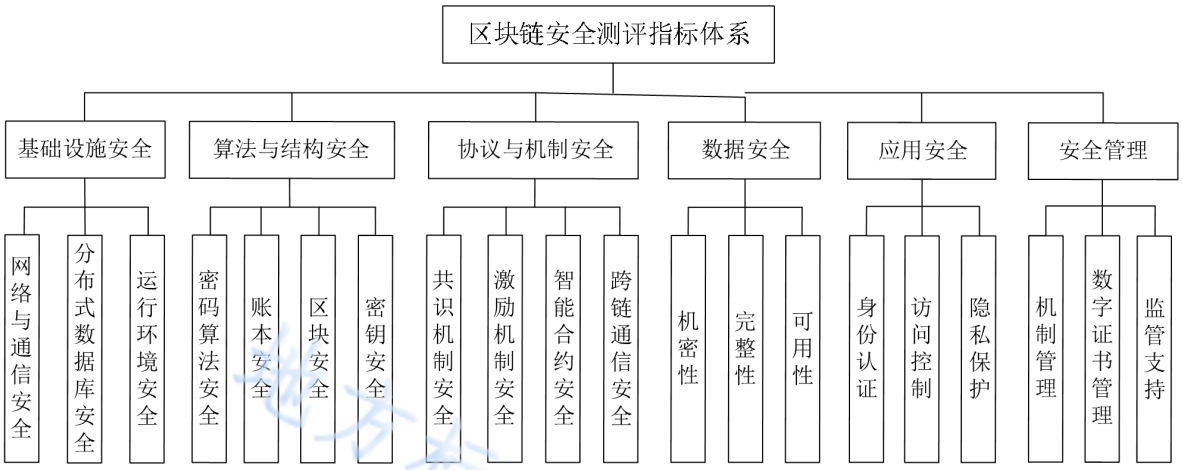

图 2　区块链安全测评指标体系

5　安全测评指标

5.1　基础设施安全

5.1.1　网络与通信安全要求如下：

a)　应保证网络设备的业务处理能力达到规定的阈值；

b)　网络节点的监控能力应达到及时发现和抵抗网络攻击的要求。

5.1.2　分布式数据库安全要求如下：

a)　应具备检测和防御各种攻击行为的能力；

b)　应保证数据交互过程中的高效性和隐私性；

c)　应具有修复损坏数据的能力。

5.1.3 运行环境安全要求如下：

a) 应具备防范入侵的能力；
b) 应具备防范恶意代码的能力；
c) 应具备处理漏洞和防范风险的能力。

5.2 算法与结构安全

5.2.1 密码算法要求如下：

a) 应支持国际主流密码算法和我国商密算法，如 AES、RSA、ECC、SM2、SM3、SM4、SM9 等；
b) 应具备抵御破解的能力，定期审核加密算法的安全性；
c) 应满足参数配置和生成过程、随机数的使用、操作模式等安全性需求。

5.2.2 账本安全要求如下：

a) 应具备持久化存储账本记录的能力，保证数据的可追溯性；
b) 应保证各个节点能对正确的账本进行同步；
c) 应具备向获得授权者提供真实数据的能力。

5.2.3 区块安全要求如下：

a) 区块应通过健壮的激励机制形成；
b) 区块应具备抵抗攻击的能力。

5.2.4 密钥安全要求如下：

a) 应具有明确的密钥管理方案；
b) 密钥应安全生成、导入和存储；
c) 密钥应能够正确、有效、安全备份；
d) 应具有密钥找回功能；
e) 应提供密钥撤销机制。

5.3 协议与机制安全

5.3.1 共识机制安全要求如下：

a) 正常运行的节点的请求应能在规定时间内达成正确、一致的共识；
b) 不超过理论值的节点数故障应不影响整个系统正常工作；
c) 每一参与节点应具有独立判断能力；
d) 共识方案的发布应具备清晰的应用场景和规模参数；
e) 在理论值范围内的恶意节点发出恶意请求时，系统应能够做出正确的响应，保证一致性。

5.3.2 激励机制安全要求如下：

a) 应保证激励发行和分配过程的公平性；
b) 应考虑通信成本、网络维护成本以及计算资源消耗成本；
c) 应设置对节点恶意行为的惩罚机制。

5.3.3 智能合约安全要求如下：

a) 智能合约开发应标准化、规范化；
b) 智能合约代码应能够进行安全性测试；
c) 智能合约代码审计验证应标准化、规范化；
d) 应建立智能合约安全漏洞信息平台；
e) 智能合约应不可被恶意篡改。

5.3.4 跨链通信安全要求如下：

a) 应保持分布式网络里节点之间连接状态的强健性；

b) 应建立统一的跨链通信数据共享所需的数据格式和通信协议；
c) 应抵御跨链间的各种攻击。

5.4 数据安全

5.4.1 机密性要求如下：
a) 数据存储应具备机密性；
b) 数据传输应具备机密性。
5.4.2 完整性要求如下：
a) 数据存储应具备完整性；
b) 数据传输应具备完整性。
5.4.3 可用性要求如下：
a) 授权主体在需要数据时应能及时得到服务；
b) 应具备数据的备份和恢复能力。

5.5 应用安全

5.5.1 身份认证要求如下：
a) 应具备用户注册、更改与注销等功能；
b) 认证信息应以密文存储和传输；
c) 应具有账户安全警告、锁定、找回功能；
d) 用户信息应与个人真实身份具有关联性。
5.5.2 访问控制要求如下：
a) 应具有对不同级别的用户授予不同权限的功能；
b) 应具有根据需要来更改系统内容的访问等级与用户的访问权限等级的功能；
c) 应避免单一权威机构的权限垄断。
5.5.3 隐私保护要求如下：
a) 用户的隐私信息不得以明文传输、存储；
b) 应将数据分为多个隐私等级；
c) 应对系统中关键数据的隐私进行保护。

5.6 安全管理

5.6.1 机制管理要求如下：
a) 应建立相应的人员管理制度；
b) 应建立软、硬件维护的管理制度；
c) 应建立区块链系统及应用的安全评估制度；
d) 应建立区块链系统及应用的安全审计制度。
5.6.2 数字证书管理要求如下：
a) 应具有完善的安全审计、流程监控、容灾备份、事故快速反应与处理等安全机制；
b) 密钥应加密存储在密钥数据库或硬件内，并以高等级的物理安全措施保护；
c) 数字证书的颁发、管理与撤回等应有相应的安全机制。
5.6.3 监管支持要求如下：
a) 应提供监管机制；
b) 应具有责任认定、责任追究机制。