ICS 35.030
L 80

团 体 标 准

T/ISEAA XXX-2022

信息安全技术
网络安全等级保护区块链安全扩展要求

Information security technology—

Blockchain system extension requirements for classified protection of cybersecurity

（草案稿）

20XX -XX-XX 发布　　20XX -XX-XX 实施

中关村信息安全测评联盟 发布

目　　录

前　言

本文件按照GB/T1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中关村信息安全测评联盟团体标准委员会提出并归口。

本文件起草单位：公安部信息安全等级保护评估中心、中国移动通信有限公司研究院、华为技术有限公司、长春吉大正元信息技术股份有限公司、绿盟科技集团股份有限公司、北方实验室（沈阳）股份有限公司、深圳市腾讯计算机系统有限公司。

本文件主要起草人：略

引　言

为了更好地适应国家区块链战略要求，应对区块链技术发展带来的安全防护需求，提升区块链系统安全的能力，增强区块链安全管理力度，《网络安全等级保护区块链安全扩展要求》依据GB/T 22239《信息安全技术 网络安全等级保护基本要求》的通用安全保护要求，提出区块链系统安全扩展要求。

本文件是网络安全等级保护相关系列标准之一，用于配合GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》使用。

与本文件相关的标准包括：

——GB/T 22240　信息安全技术　网络安全等级保护定级指南

——GB/T 22239　信息安全技术　网络安全等级保护基本要求

——GB/T 28448　信息安全技术　网络安全等级保护测评要求

信息安全技术 网络安全等级保护区块链安全扩展要求

1 范围

本文件规定了网络安全等级保护第一级至第四级区块链基础设施网络安全等级保护对象的安全扩展要求。

本文件适用于私有链安全建设及服务，也可用于指导联盟链安全建设及服务。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

3 术语和定义

GB/T 22239、GB/T 28448和GB/T 39786-2021界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

一种将数据区块顺序相连，并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

［来源：ISO 22739:2020，3.6，有修改］

3.2

区块链节点 blockchain node

具有共识机制、智能合约等特定功能的区块链组件，可独立运行的单元。

［来源：ISO 22739:2020，3.50，有修改］

3.3

区块链基础设施 blockchain infrastructure

结合对等网络、共识机制、去中心化存储等区块链核心技术，连接多个区块链节点并提供其上智能合约、共识机制等服务的软硬件集合。

3.4

区块链应用 blockchain application

基于区块链基础设施提供服务的业务应用系统。

3.5

共识机制 consensus protocol

实现不同区块链节点之间建立信任、达成一致的机制。

3.6

事务 transaction

由底层协议允许的最小且不可分割的工作单位。通常一个事务对应一个完成的业务，如转账、授权等。

3.7

智能合约 smart contract

基于预定事件触发和自动执行的计算机程序，是对现实中合约条款执行电子化的量化事务协议，其执行结果记录在分布式账本中。

［来源：ISO 22739:2020，3.72，有修改］

3.8

公有链 public blockchain

任意区块链节点均可接入，所有接入区块链节点均可参与共识和读写数据的一类区块链部署模型。

3.9

联盟链 consortium blockchain

由一组用户授权的区块链点可接入，接入节点可按规则参与共识和读写数据的区块链部署模型。

3.10

私有链 private blockchain

由单个用户授权的区块链点可接入，接入节点可按规则参与共识和读写数据的区块链部署模型。

4 缩略语

下列缩略语适用于本文件。

PKI：公钥基础设施（Public Key Infrastructure）

RPC：远程过程调用（Remote Procedure Call）

SDK：软件开发工具包（Software Development Kit）

5 概述

根据GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》给出的定级对象基本特征，区块链基础设施等级保护对象是结合对等网络、共识机制、去中心化存储等区块链核心技术，连接多个区块链节点并提供其上智能合约、共识机制等服务的软硬件集合。

区块链节点具有共识机制、智能合约等特定功能的区块链组件，可独立运行的单元。区块链节点可抽象为资源层、核心层和接口层。区块链应用是采用区块链基础设施提供服务的业务应用系统。区块链基础设施及区块链应用的架构关系如图1所示。

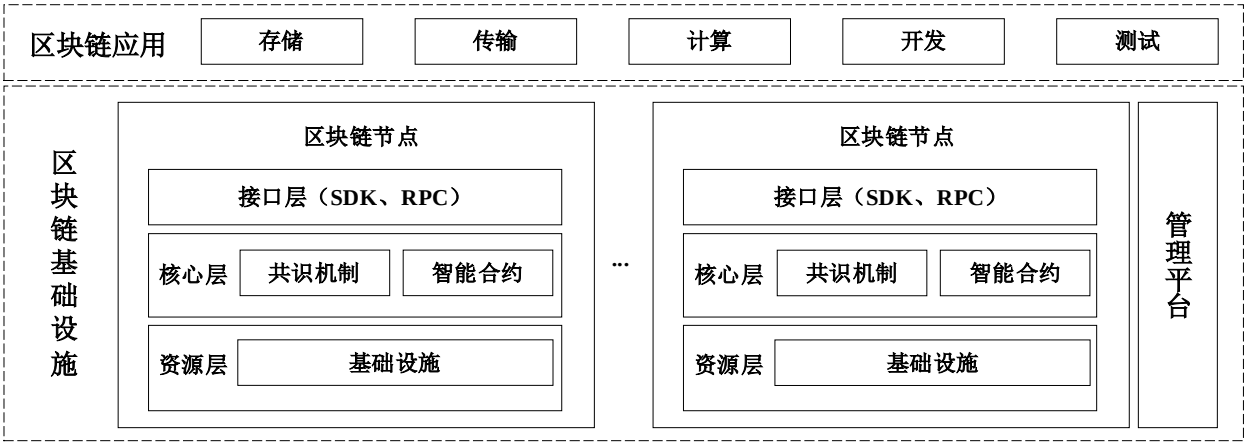

图1　区块链基础设施及区块链应用的架构关系

在区块链节点中，资源层提供区块链运行所需要的物理服务器、虚拟机以及容器等基础资源；区块链节点上可能运行共识机制和智能合约的一种或多种；核心层包括共识机制、智能合约等多种区块链核心功能；接口层对区块链应用屏蔽底层细节，形成高效易用的、标准化的开发接口，以 SDK、RPC 等方式提供服务。

6　第一级安全扩展要求

6.1 安全物理环境

6.1.1 基础设施位置

应保证承载区块链基础设施的设备机房位于中国境内。

6.2 安全通信网络

6.2.1 网络架构

应保证区块链基础设施不承载高于其安全保护等级的区块链应用和业务。

6.2.2 对等网络安全

本项要求包括：

a)　应提供白名单等节点身份验证机制进行节点接入限制；

b)　应保证离线节点重新加入系统后，能够进行数据同步。

6.3 安全计算环境

6.3.1 数据完整性

交易与账本应在多节点拥有完整的数据记录并确保各节点数据的一致性。

7　第二级安全扩展要求

7.1 安全物理环境

7.1.1 基础设施位置

应保证承载区块链基础设施的设备机房位于中国境内。

7.2 安全通信网络

7.2.1 网络架构

应保证区块链基础设施不承载高于其安全保护等级的区块链应用和业务。

7.2.2 对等网络安全

本项要求包括：

a) 应提供白名单等节点身份验证机制进行节点接入限制；
b) 应保证离线节点重新加入系统后，能够进行数据同步；
c) 应采用动态配置节点通信的组网方式，避免单点故障影响整个区块链网络通信。

7.3 安全计算环境

7.3.1 身份鉴别

应采用校验或密码技术对区块链节点进行身份鉴别。

7.3.2 访问控制

本项要求包括：

a) 应建立接口层访问控制策略，严格限制不同类型用户对区块链基础设施资源的读取、写入等访问权限；
b) 应启用接口层登录失败处理功能，例如结束会话、限制非法登录次数和超时自动退出等功能。

7.3.3 安全审计

本项要求包括：

a) 应具备对智能合约的部署和运行的审计能力；
b) 应对智能合约进行安全性审计，并保留审计记录。

7.3.4 智能合约

本项要求包括：

a) **应对用户提供智能合约安全写作规范，并建设智能合约安全检查机制；**
b) **应对用户上传的智能合约进行基础安全检测，包括智能合约基线安全检测、框架性安全检测等，并将检测结果和风险情况告知上传用户；**
c) **应提供智能合约安全开发规范，遵循相关合约在运行安全、接口安全、安全配置等方面的开发安全要求；**
d) **应具备对访问智能合约用户的身份鉴别和访问控制机制。**

7.3.5 共识安全

应披露共识算法类型、同步网络模型，容错条件以及适用场景。

7.3.6 数据完整性

交易与账本应在多节点拥有完整的数据记录并确保各节点数据的一致性。

7.3.7 数据保密性

应确保账本数据中用户隐私数据的安全存储，防止未授权读取和篡改。

7.4 安全运维管理

7.4.1 密码管理

本项要求包括：

a) **使用密码算法、技术、产品及服务，应符合国家密码管理部门及行业标准规范要求；**

b) **采用的密码产品应达到GB/T 37092《信息安全技术 密码模块安全要求》一级及以上安全要求。**

7.4.2 密钥管理

密钥管理应符合GB/T 39786《信息安全技术 信息系统密码应用基本要求》。

8 第三级安全扩展要求

8.1 安全物理环境

8.1.1 基础设施位置

应保证承载区块链基础设施的设备机房位于中国境内。

8.2 安全通信网络

8.2.1 网络架构

本项要求包括：

a) 应保证区块链基础设施不承载高于其安全保护等级的区块链应用和业务；

b) **应保证区块链基础设施具备节点身份管理及准入控制，防止恶意节点加入区块链基础设施。**

8.2.2 对等网络安全

本项要求包括：

a) 应提供**PKI证书**等节点身份验证机制进行节点接入限制；

b) 应保证离线节点重新加入系统后，能够进行数据同步；

c) 应采用动态配置节点通信的组网方式，避免单点故障影响整个区块链网络通信；

d) **应保证通信过程的双向认证和授权。**

8.3 安全计算环境

8.3.1 身份鉴别

应采用**密码**技术对区块链节点进行身份鉴别。

8.3.2 访问控制

本项要求包括：

a) 应建立接口层访问控制策略，严格限制不同类型用户对区块链基础设施资源的读取、写入等访问权限；

b) 应启用接口层登录失败处理功能，例如结束会话、限制非法登录次数和超时自动退出等功能；
c) 应采用密码技术手段确保数据在传输过程中的完整性和保密性；
d) 应依照“最小应知”原则向用户开放访问授权。

8.3.3 安全审计

本项要求包括：
a) 应具备对智能合约的部署和运行的审计能力；
b) 应对智能合约进行安全性审计，并保留审计记录；
c) 应对链上数据的更新、删除、所属权变更等操作进行记录，提供可追溯能力。

8.3.4 智能合约

本项要求包括：

a) 应对用户提供智能合约安全写作规范，并建设智能合约安全检查机制；

b) 应对用户上传的智能合约进行基础安全检测，包括智能合约基线安全检测、框架性安全检测等，并将检测结果和风险情况告知上传用户；

c) 应提供智能合约安全开发规范，遵循相关合约在运行安全、接口安全、安全配置等方面的开发安全要求；

d) 应具备对访问智能合约用户的身份鉴别和访问控制机制；

e) **应具备智能合约的仲裁响应机制，可在仲裁后执行智能合约冻结和恢复等相关措施；**

f) **应通过自提供的智能合约代码审计功能或支持第三方代码审计等方式，对用户上传的智能合约进行必要的代码审计。**

8.3.5 共识安全

本项要求包括：

a) 应披露共识算法类型、同步网络模型，容错条件以及适用场景；

b) **共识算法应支持共识节点动态缩容、扩容；**

c) **共识机制应具有容错性及一致性，具备防重放攻击的能力；**

d) **应保证共识节点正常重启，或共识节点从异常场景恢复后，共识节点可正常参与共识和同步数据，保证各节点数据一致。**

8.3.6 数据完整性

交易与账本应在多节点拥有完整的数据记录并确保各节点数据的一致性。

8.3.7 数据保密性

本项要求包括：
a) 应确保账本数据中用户隐私数据的安全存储，防止未授权读取和篡改；
b) 应针对账本数据和状态数据的查询和操作采用认证授权等访问控制技术进行限制，防止未授权读取和篡改。

8.4 安全管理中心

8.4.1 集中管控

本项要求包括：

a) 应具备对链的业务资源监控功能，包括事务数量、合约数量以及事务队列数量等；

b) 应具备对链上所有区块链节点的业务资源监控功能，包括区块链节点发起事务或合约、验证事务或合约等。

8.5 安全运维管理

8.5.1 密码管理

本项要求包括：

a) 使用密码算法、技术、产品及服务，应符合国家密码管理部门及行业标准规范要求；

b) 采用的密码产品应达到GB/T 37092《信息安全技术 密码模块安全要求》**二级**及以上安全要求。

8.5.2 密钥管理

密钥管理应符合GB/T 39786《信息安全技术 信息系统密码应用基本要求》。

9 第四级安全扩展要求

9.1 安全物理环境

9.1.1 基础设施位置

应保证承载区块链基础设施的设备机房位于中国境内。

9.2 安全通信网络

9.2.1 网络架构

本项要求包括：

a) 应保证区块链基础设施不承载高于其安全保护等级的区块链应用和业务；

b) 应保证区块链系统具备节点身份管理及准入控制，防止恶意节点加入区块链系统。

9.2.2 对等网络安全

本项要求包括：

a) 应提供PKI证书等节点身份验证机制进行节点接入限制；

b) 应保证离线节点重新加入系统后，能够进行数据同步；

c) 应采用动态配置节点通信的组网方式，避免单点故障影响整个区块链网络通信；

d) 应保证通信过程的双向认证和授权。

9.3 安全计算环境

9.3.1 身份鉴别

应采用密码技术对区块链节点进行身份鉴别。

9.3.2 访问控制

本项要求包括：

a) 应建立接口层访问控制策略，严格限制不同类型用户对区块链基础设施资源的读取、写入等访问权限；
b) 应启用接口层登录失败处理功能，例如结束会话、限制非法登录次数和超时自动退出等功能；
c) 应采用密码技术手段确保数据在传输过程中的完整性和保密性；
d) 应依照“最小应知”原则向用户开放访问授权。

9.3.3 安全审计

本项要求包括：

a) 应具备对智能合约的部署和运行的审计能力；
b) 应对智能合约进行安全性审计，并保留审计记录；
c) 应对链上数据的更新、删除、所属权变更等操作进行记录，提供可追溯能力。

9.3.4 智能合约

本项要求包括：

a) 应对用户提供智能合约安全写作规范，并建设智能合约安全检查机制；
b) 应对用户上传的智能合约进行基础安全检测，包括智能合约基线安全检测、框架性安全检测等，并将检测结果和风险情况告知上传用户；
c) 应提供智能合约安全开发规范，遵循相关合约在运行安全、接口安全、安全配置等方面的开发安全要求；
d) 应具备对访问智能合约用户的身份鉴别和访问控制机制；
e) 应具备智能合约的仲裁响应机制，可在仲裁后执行智能合约冻结和恢复等相关措施；
f) 应通过自提供的智能合约代码审计功能或支持第三方代码审计等方式，对用户上传的智能合约进行必要的代码审计。

9.3.5 共识安全

本项要求包括：

a) 应披露共识算法类型、同步网络模型，容错条件以及适用场景；
b) 共识算法应支持共识节点动态缩容、扩容；
c) **应选择可证明安全的共识机制**，共识机制应具有容错性及一致性，具备防重放攻击的能力；
d) 应保证共识节点正常重启，或共识节点从异常场景恢复后，共识节点可正常参与共识和同步数据，保证各节点数据一致。

9.3.6 数据完整性

交易与账本应在多节点拥有完整的数据记录并确保各节点数据的一致性。

9.3.7 数据保密性

本项要求包括：

a) 应确保账本数据中用户隐私数据的安全存储，防止未授权读取和篡改；

b) 应针对账本数据和状态数据的查询和操作采用认证授权等访问控制技术进行限制,防止未授权读取和篡改。

9.4 安全管理中心

9.4.1 集中管控

本项要求包括：

a) 应具备对链的业务资源监控功能，包括事务数量、合约数量以及事务队列数量等；

b) 应具备对链上所有区块链节点的业务资源监控功能，包括区块链节点发起事务或合约、验证事务或合约等。

9.5 安全运维管理

9.5.1 密码管理

本项要求包括：

a) 使用密码算法、技术、产品及服务，应符合国家密码管理部门及行业标准规范要求；

b) 采用的密码产品应达到GB/T 37092《信息安全技术 密码模块安全要求》**三级及**以上安全要求。

9.5.2 密钥管理

密钥管理应符合GB/T 39786《信息安全技术 信息系统密码应用基本要求》。