ICS 35.240.01
CCS L 80

团　　体　　标　　准

T/CESA 1221—2022

区块链 专用服务网络

基础设施总体要求

Blockchain—Private service network—General requirements

for infrastructure

2022-08-29 发布　　2022-09-29 实施

中国电子工业标准化技术协会　发布

目　　次

前　言

本文件按照GB/T 1.1—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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由国家信息中心提出。

本文件由中国电子工业标准化技术协会归口。

本文件起草单位：国家信息中心、中国移动通信集团设计院有限公司、中国银联股份有限公司、北京红枣科技有限公司、深圳前海微众银行股份有限公司、湖北省发展和改革委员会、重庆江北区大数据应用发展管理局、重庆市区块链数字经济产业园管委会、长春政务服务和数字化建设管理局、长春市信息中心、长沙市数据资源管理局、中国移动通信有限公司政企客户分公司、中国移动通信集团重庆有限公司、中国移动通信集团湖北有限公司、中国移动通信集团甘肃有限公司、中国移动通信集团浙江有限公司杭州分公司、中国移动通信集团宁夏有限公司、中国移动通信集团江苏有限公司、中国移动通信集团海南有限公司、中国移动通信集团河北有限公司、中国移动通信集团吉林有限公司、中国移动通信集团湖南有限公司长沙分公司、海南火链科技有限公司、中国雄安集团数字城市科技有限公司、苏州市相城区块链科技有限公司、北京国信恒达智慧城市科技发展有限公司、易盾链动（重庆）数字科技有限公司、北京泰豪智能工程有限公司、北京百度网讯科技有限公司。

本文件主要起草人：单志广、高鹏、谭敏、何亦凡、许玉壮、邓伟平、李贺、代翔、郎晓夫、张高山、詹义、杨鹏、费光荣、魏飞、马晓军、刘国栋、张延强、陈栩、唐斯斯、马潮江、戴彧、王丹丹、闫晓丽、涂菲菲、朱华、倪宁宁、刘仲思、咸燕、范瑞彬、张开翔、吴芸、肖竞佳、石飞前、邓永俊、于本江、李欣、庄毅、王也、丁慧东、赵哲、柳羽辉、叶亭吟、罗斌、何青阳、张程、刘焱宇、吴波、饶毅、贾奋勇、张磊、张明明、王文生、屠宇飞、柳毅、朱智俊、童洲游、段立、吴东平、张峻岭、杨鹏、孙思远、许慧莹、邢维年、刘克飞、刘爱华、张文璇、刘云龙、毕纪伟、田洪峰、初航、牛奔、邵林、唐晖、杨威、陈川、陈杰、王悦晞、郑立峰、姚彬、刘俊杰、曾德华、万玮、邢立立、刘广斌、肖伟。

区块链 专用服务网络 基础设施总体要求

1 范围

本文件规定了区块链专用服务网络基础设施的总体要求，包括基础层、支撑层、接入层、应用层、安全体系、与外部节点的数据交换、运行维护、监管机制等方面。

本文件适用于指导政府、事业和企业单位等开展专用网络环境中区块链系统的建设和服务运营。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 32905-2016 信息安全技术 SM3密码杂凑算法

GB/T 32907-2016 信息安全技术 SM4分组密码算法

GB/T 32918.2-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32918.3-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

GM/T 0045-2016 金融数据密码机技术规范

GM/T 0054-2018 信息系统密码应用基本要求

GM/T 0059-2018 服务器密码机检测规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块 block

一种包含区块头和区块数据的数据结构。

注：区块头包含前一个区块的摘要信息。

3.2

共识 consensus

在分布式节点间达成区块数据一致性的认可。

3.3

共识机制 consensus mechanism

在分布式节点间达成共识（3.2）的规则和程序。

3.4

共识算法 consensus algorithm

在分布式节点间为达成共识（3.2）而采用的计算方法。

3.5

分布式账本 distributed ledger

在分布式节点间共享并使用共识机制（3.3）实现具备一致性的账本。

3.6

区块链 blockchain

使用密码技术链接将共识确认过的区块（3.1）按顺序追加形成的分布式账本（3.5）。

3.7

区块链专用服务网 blockchain private service network

区块链专网

在专线传输的内网或局域网内，搭建包括底层区块链（3.6）网络、配套的管理平台、运维平台和应用门户等在内的一整套区块链（3.6）应用运行的基础设施。

3.8

智能合约 smart contract

存储在分布式账本（3.5）中的计算机程序，其共识（3.2）执行结果都记录在分布式账本（3.5）中。

3.9

对等网络 peer-to-peer network

一种仅包含对控制和操作能力等效节点的计算机网络。

3.10

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量，输入参量通常被称为密钥。

3.11

虚拟专用网络 virtual private network

在公用网络上建立专用网络，进行加密通讯。

3.12

跨链技术 inter-blockchain technology

实现多个区块链（3.6）或分布式账本（3.5）之间信息交换的技术集合。

3.13

节点 node

提供专网中所有功能或部分功能的服务器。

3.14

记账节点 committer node

负责账本数据完整性的节点。

3.15

共识节点 consensus node

负责账本数据一致性的节点。

3.16

交易验证节点 transaction verification node

负责对提交的交易数据进行验证的节点。

3.17

节点标识 node identification

唯一标识一个区块链节点，实现对区块链节点的寻址。

3.18

标识鉴别信息 identification information

系统正确识别节点身份的重要途径。

3.19

访问控制 access control

防止对任何资源进行未授权的访问，使系统在合法的范围内使用。

3.20

身份标识 identification

用来证明身份的凭证。

3.21

隐私 privacy

不愿意或不便于为第三方知道的信息或侵入的领域，与他人或社会利益无关。

3.22

源链 source chain

跨链时主动发起跨链操作的链。

3.23

目标链 destination chain

跨链时跨链合约的被执行链。

3.24

公共节点 common node

部署在专网环境内部云资源中的公共区块链（3.6）环境。
注：记账节点（3.14）的资源池，每个公共节点内包含多个记账节点（3.14）。

3.25

外部节点 external node

区块链专网环境之外的区块链（3.6）记账节点（3.14）。

4 缩略语

下列缩略语适用于本文件。
AES 高级加密标准（Advanced Encryption Standard）
API 应用编程接口（Application Programming Interface）
CA 数字证书认证机构（Certificate Authority）
DES 数据加密标准（Data Encryption Standard）
DoS 磁盘操作系统（Disk Operating System）
ECC 椭圆曲线加密（Elliptic Curve Cryptography）
HTTPS 超文本传输安全协议（Hyper Text Transfer Protocol over SecureSocket Layer）
PKI 公钥基础设施（Public Key Infrastructure）
TPS 每秒事务处理量（Transaction PerSecond）
SDK 软件开发工具包（Software Development Kit）
VPN 虚拟专用网络（Virtual Private Network）

5 通用要求和总体框架

5.1 通用要求

5.1.1 兼容性要求

区块链专网运行环境的兼容性，应符合以下要求：
a） 运行环境兼容现有主流的Linux操作系统和网络运行环境；
b） 兼容多种主流的开源联盟链底层框架；
c） 具有多种主流区块链共识机制；
d） 支持多种主流开发语言的智能合约。

5.1.2 可扩展要求

区块链专网运行环境的可扩展性，应符合以下要求：
a） 基础层环境资源具备动态扩展能力，当运行资源不足时，能在不影响系统正常运行的情况下进行动态资源扩展；
b） 实现对区块链底层框架、加密算法和共识机制的可插拔式扩展。

5.1.3 安全性要求

区块链专网运行环境的安全性，应符合以下要求：

a） 遵循GB/T 22239-2019 中的第三级安全要求；

b） 具备支持SM2、SM3、secp256K1、ECC、RSA等多种主流密码算法的能力。

5.1.4 可管理要求

区块链专网运行环境的可管理性，应满足以下要求：

a） 区块链专网具备对分布式账本节点、区块链应用的管理功能，包括事件管理、问题管理、安全管理、监控管理等；

b） 区块链专网具备统一身份认证、授权和鉴权管理功能。

5.2 总体框架

区块链专用服务网络基础设施的各部分组成及基本逻辑关系，见图1。

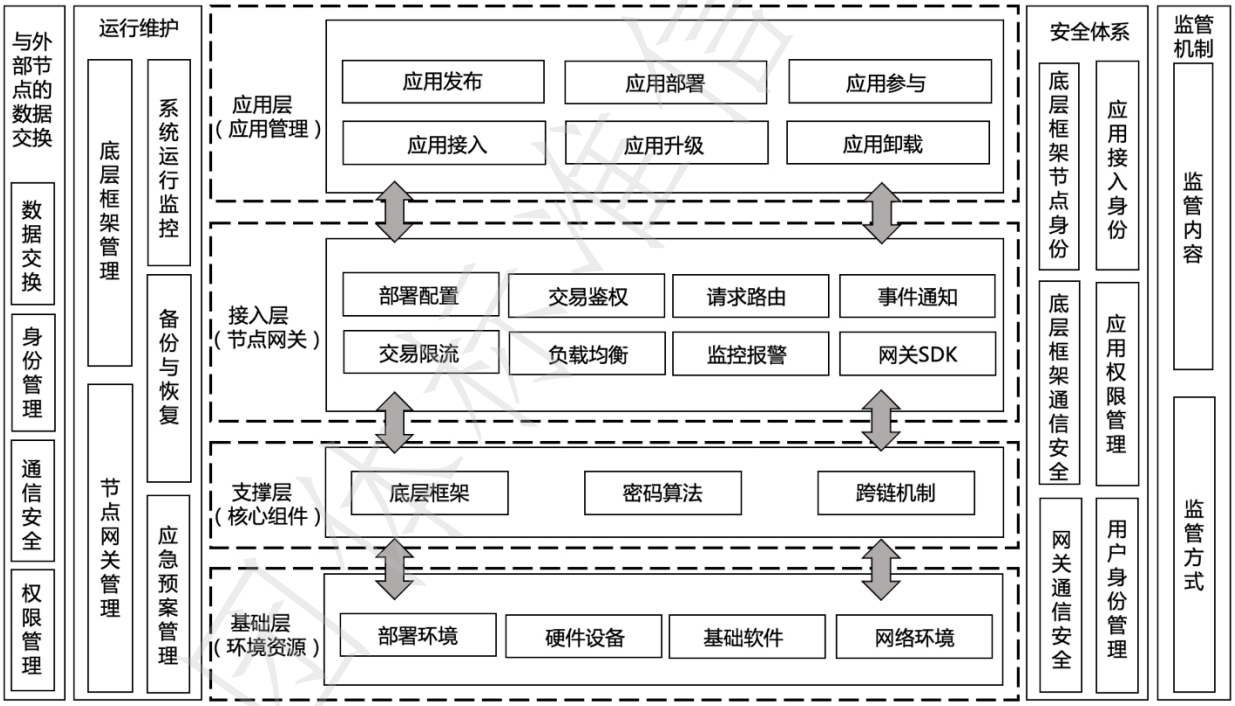

图1 区块链专用服务网络基础设施框架

依据图1，提出了以下基础设施要求：

a） 基础层（环境资源）：指对于区块链专网的运行环境的要求，包括部署环境要求、硬件设备要求、基础软件要求以及网络环境要求；

b） 支撑层（核心组件）：指对于区块链专网中底层框架、密码算法、跨链机制等核心功能组建的要求。其中，底层框架包括共识机制要求、智能合约要求、账本管理要求、对等网络要求以及应用服务隔离要求；密码算法包括非对称加密算法要求、对称加密算法要求、数据哈希算法要求、对称加密算法要求、加密方法要求以及密钥管理要求；跨链机制包括跨链技术要求以及数据安全要求等；

c） 接入层（节点网关）：指对于区块链专网中节点接入网关的要求，包括节点网关部署配置要求、交易鉴权要求、请求路由要求、事件通知要求、交易限流要求、负载均衡要求、监控报警要求以及网关SDK要求；

d） 应用层（应用管理）：指对于区块链专网中应用管理的要求，包括应用发布要求、应用部署要求、应用参与要求、应用接入要求、应用升级要求以及应用卸载要求；
e） 安全体系：指对于区块链专网中安全体系的要求，包括底层框架节点身份要求、底层框架通信安全要求、网关通信安全要求、应用接入身份要求、应用权限管理要求以及用户身份管理要求；
f） 与外部节点的数据交换:指对于区块链专网与外部节点的数据交换要求，包括外部节点数据交换要求、身份管理要求、通信安全要求以及权限管理要求；
g） 隐私保护：指对于区块链专网中隐私保护的要求，包括隐私保护的原则、内容、策略、技术以及监控、审计要求；
h） 运行维护：指对于区块链专网中运行维护的要求，包括底层框架管理要求、节点网关管理要求、系统运行监控要求、备份与恢复要求以及应急预案管理要求；
i） 监管机制：指对于区块链专网中监管机制的要求，包括监管内容要求以及监管方式要求。

6 基础层

6.1 部署环境要求

区块链专网运行环境资源部署，应符合以下要求：
a） 支持在已有的内网或局域网资源环境中搭建运行环境；
b） 以TCP/IP为基础进行网络资源传输；
c） 支持公有云、私有云等多云环境资源适配。

6.2 硬件设备要求

6.2.1 场地安全

区块链专网运行环境资源的场地安全，应符合以下要求：
a） 为设备提供安全、高速、稳定的运行机房，同时对机房环境进行实时监测；
b） 对于云端部署模式，保证数据中心运行环境位于高安全区域；
c） 保证区块链专网使用者业务运行、数据存储和处理设备位于中国境内。

6.2.2 硬件设备

区块链专网运行环境资源的硬件设备，应符合以下要求：
a） 对设备运行状态、资源使用情况等进行监控，能在发生异常情况时发出告警；
b） 网络硬件满足所支持数据系统的传输速率要求；
c） 网络的存储及备份能够实现冗余，以便在出现故障时保障系统正常运行。

6.2.3 硬件加密设备安全

硬件加密设备安全应支持硬件加密设备的接入，使用加密机设备应符合GM/T 0045-2016标准中的金融数据密码机硬件要求、安全性要求。

6.3 基础软件要求

6.3.1 公共节点平台

区块链专网基础软件应包括公共节点平台，且应符合以下要求：
a） 支持跨多个区块链底层框架；

b） 支持多应用链的独立运行，且保证隐私隔离；
c） 具备智能合约自动化编译、测试、部署机制；
d） 支持区块链应用之间的跨链数据互通；
e） 支持节点资源的热部署；
f） 具备节点资源动态分配的能力。

6.3.2 账本结构

账本结构宜使用块链式或近块链式的存储结构，应使用哈希嵌套等手段防止数据被篡改。

6.3.3 分布式组网

分布式组网应由分布在逻辑或物理上不同位置的节点互连而成，任一节点应至少与其他两个节点建立通信连接。

6.3.4 数据存储

数据存储应根据数据对象的类别独立存储；账户数据、交易数据、配置数据及账本元数据等应分别管理、分别操作。

6.4 网络环境要求

区块链专网运行网络环境，应符合以下要求：
a） 区块链专网应在基于内网或局域网的服务基础设施上部署，包括分布式账本节点、区块链底层框架以及共识机制等；
b） 在网络拓扑中，应防止单个节点故障而造成网络隔离；
c） 具备一定的网络管理手段，能够合理配置和调整网络负载，监视网络状态。

7 支撑层

7.1 底层框架

7.1.1 共识机制

区块链专网底层框架的共识机制，应符合以下要求：
a） 多共识机制：专网内区块链支持基于不同联盟链底层框架的多种共识机制选择；
b） 数据一致性：支持多节点对链上数据的记录、验证、修改等操作达成共识，使参与节点的账本在所有区块中数据都是一致的，且执行区块中的交易后得到的最终状态也是一致的；防止任何独立节点恶意修改链上数据；
c） 容错性：保证故障节点和恶意节点的比例不超过共识机制容错率时，系统能正常运行；
d） 公平性：在共识机制的规则约束下，恶意节点无法通过技术手段无限提高出块比例，或者干扰降低其他共识节点的出块比例，保证链上公平性；
e） 可升级性：共识算法的关键参数（如出块周期、加入和退出的条件、新区块的奖励规则等）通过投票表决的方法完成热升级，避免出现网络的硬分叉。

7.1.2 智能合约开发运行环境

7.1.2.1 开发环境要求

区块链专网底层框架的智能合约开发环境，应符合以下要求：

a） 支持使用多种智能合约开发语言，包括但不限于Java、Python、NodeJs、Golang、Solidity等，应提供配套的集成开发环境；
b） 外部数据源的影响范围仅限于智能合约范围内，不影响区块链系统整体运行；
c） 支持智能合约内容静态、动态检查和自动修复。

7.1.2.2 智能合约运行要求

区块链专网底层框架的智能合约运行环境，应满足以下要求：
a） 支持基于多种联盟链底层框架的运行载体，如虚拟机等；
b） 智能合约的执行具备原子性，支持执行过程中发生错误时的回滚；
c） 智能合约的执行具备一致性，包括执行结果完全相同且多个节点同时执行合约时，保证数据的完整性且数据同步互不干扰；
d） 支持智能合约安全升级，保证原合约数据的可信迁移；
e） 支持智能合约的版本管理，在源代码、配置文件中以及部署或升级操作时定义版本号，并保留历史版本，交易信息中明确调用的智能合约版本；
f） 支持合约隔离，不同的合约之间，以及同一个合约的多次调用之间是资源隔离的，不会因为少数调用消耗大量资源而影响整个系统的可用性；
g） 支持智能合约可控性，合约请求执行过程是可终止的。

7.1.3 账本管理

区块链专网底层框架应支持账本管理，且应符合以下要求：
a） 多底层框架适配：具备专网内对多个联盟链底层框架下不同账本的管理能力；
b） 可监管性：支持账本数据的监管审计，监管内容包括数据的记录日期、时间、用户标识、数据内容等；
c） 可追溯性：对任意一个账本上的区块，可以回溯到它之前的区块；对于一笔交易，可以回溯到其资金的来源；对于一个合约调用，可以回溯到调用生效前合约变量的版本和状态；
d） 安全性：保护账本数据的安全，防止其被未授权的第三方非法获取；保护系统和网络安全，防止单节点崩溃造成严重的数据丢失；
e） 可验证性：对于已经上链的交易，用户得到一个出示给相关方的轻量级节点证明，在不存储全账本的情况下验证交易是否已经上链；
f） 完整性：保障账本数据的完整性，防止其被恶意篡改或破坏；
g） 可拓展性：底层的存储引擎具备可扩展性，支持从单块硬盘扩展到多块盘、从单机存储扩展到分布式云存储。

7.1.4 对等网络

区块链专网底层框架应支持对等网络，且应符合以下要求：
a） 多协议支持：支持在多种联盟链底层框架下，基于libp2p模式和gRPC模式的多种对等网络通信协议；
b） 自发现：节点需要有自发现能力，通过连接网络中的少数种子节点同步到整个网络中足够多的节点，且快速发现邻居节点的上下线，并及时地更新连接路由表；
c） 安全通信：支持节点之间高效安全的通信；节点之间的通信采用TLS协议或类似的加密连接；通信密钥与区块链上的交易认证密钥需要分离；具有多播能力。

7.1.5 应用服务隔离

区块链专网底层框架应支持应用服务隔离，且应符合以下要求：

a） 支持多个联盟链底层框架下同构和异构区块链应用的隔离；
b） 不同应用的账本数据保证独立性，对某一账本的操作不影响其他账本的状态；
c） 应用部署和调用的智能合约仅能对其相关的账本数据进行操作；
d） 应用发起的交易提案只有相关节点接收到相关交易的信息，且与其他应用完全隔离。

7.2 密码算法

7.2.1 非对称加密算法

专网应具备支持SECP256k1、SECP256r1以及SM2椭圆曲线密码算法等非对称加密算法的能力。

7.2.2 数据哈希算法

专网应具备支持SHA-1、SHA-3、RSA算法以及国密SM3散列算法等数据哈希算法的能力。

7.2.3 对称加密算法

专网应具备支持DES、3DES、AES和国产SM4加密算法等对称加密算法的能力。

7.2.4 加密方法

7.2.4.1 硬件加密

使用的加密机等设备应符合GM/T 0059-2018和GM/T 0045-2016等标准对密码机类密码设备的检测要求，所有加密算法都应通过硬件运算实现，应采用密码卡（二级及以上）。

密码机生成的加密算法同时应符合GB/T 32905-2016对SM3密码杂凑算法的要求、应符合GB/T 32907-2016对SM4分组密码算法的要求、应符合GB/T 32918.2-2016对SM2椭圆曲线公钥密码算法的要求。

7.2.4.2 云加密

云加密密码设备属于硬件密码模块，所有加密算法都应通过硬件运算实现，应采用密码卡（二级及以上）。

使用安全API供外围调用时应保证接口调用通讯和认证安全，管理接口应包括应用权限管理、应用管理、密钥管理等。

云加密密码设备生成的加密算法同时应符合GB/T 32905-2016对SM3密码杂凑算法的要求、应符合GB/T 32907-2016对SM4分组密码算法的要求、应符合GB/T 32918.2-2016 对SM2椭圆曲线公钥密码算法的要求。

7.2.5 密钥管理

分布式账本密钥管理应符合GB/T 32918.3-2016 第3部分：密钥交换协议中对密钥交换的要求，并且应符合GM/T 0054-2018标准中对密钥管理的要求。

7.3 跨链机制

7.3.1 跨链技术要求

区块链专网跨链机制应符合以下技术要求：

a） 专网支持同构链与异构链的跨链互通；
b） 跨链采用中继链架构以组件化方式实现，在源链与目标链间使用中继进行监听并传输跨链数据和跨链数据的证明信息，确保跨链数据正确，无法被伪造和篡改；

c） 不应对跨链数据格式作限制性要求；
d） 专网的跨链功能支持多种主流的开源联盟链框架。

7.3.2 数据安全要求

区块链专网跨链机制应符合以下数据安全要求：
a） 保证跨链数据的安全与隐私，通过跨链验证、算法、通信机制等技术保证跨链交互的安全性；
b） 在源链与目标链间对跨链数据进行记录、验证和归档，确保跨链数据可监管、可追溯；
c） 目标链在接收到跨链数据后，对其来源与合法性进行验证，验证通过后才能调用跨链合约。

8 接入层

8.1 部署配置

区块链专网节点网关应符合以下要求：
a） 专网中的每一个公共节点都应部署一个节点网关；
b） 提供https接口，供链下业务系统进行调用；
c） 具有管理该公共节点中用户托管的身份证书、对用户提交的交易进行验证、选择合适的记账节点提交交易等功能。

8.2 交易鉴权

区块链专网节点网关应支持交易鉴权，且应符合以下要求：
a） 在用户实际使用时对交易进行权限验证；
b） 进行身份鉴权认证，可根据用户提交的交易信息实现身份认证和授权；
c） 在保证访问安全的前提下进行用户权限信息的缓存。

8.3 请求路由

在公共节点中，不同的应用部署在不同底层框架所对应的各自节点中，专网的节点网关应根据实际需要访问应用和应用的部署信息，并且动态选择正确的节点进行交易。

8.4 事件通知

区块链专网节点网关需要监听应用内智能合约产生的事件，根据应用中注册的关键字进行筛选和通知，并主动通知相关用户。

8.5 交易限流

区块链专网节点网关应具备对应用使用的TPS、磁盘容量、网络流量等进行统计，并根据应用配置调节TPS和网络流量。

8.6 负载均衡

区块链专网节点网关应具备负载均衡机制，实现对网络和服务器带宽、算力等资源的高效利用，提高资源的灵活性和可用性。

8.7 监控报警

区块链专网节点网关的监控报警应符合以下要求：
a） 区块链专网应具备运行监控模块，对区块链的各资源及数据进行监控，并具备预警、报警机

制；

b） 区块链专网应对各种记账节点、节点网关、区块链应用以及业务系统等日常运行情况进行实时监控，并提供完整、可视化的运行监控功能。

8.8 网关 SDK

区块链专网节点网关的SDK应符合以下要求：

a） 提供多联盟链底层框架网关的SDK；

b） 具备链外系统接入节点网关的功能；

c） 具备链上交易接口调用、本地生成公私钥对、注册用户、生成证书签名、加密解密数据等功能；

d） 提供支持不同编程语言的专网节点网关SDK，且功能相同。

9 应用层

9.1 应用发布

区块链专网的应用发布符合以下要求：

a） 发布者应提供必要的应用信息，包括但不限于基本信息、节点资源、智能合约、角色权限、接入方式等；

b） 应具备对应用信息进行审核的功能。

9.2 应用部署

区块链专网的应用部署应符合以下要求：

a） 对通过审核的应用配置相应的公共节点、TPS、带宽、存储容量等资源；

b） 具备自动部署和手动部署两种部署方式。

9.3 应用参与

区块链专网的应用参与符合以下要求：

a） 应提供参与应用的功能，至少支持邀请加入和申请加入两种方式；

b） 应为应用发布者提供参与应用审核的功能，对申请加入的参与者进行审核；

c） 宜提供应用市场或精选应用等应用展示功能。

9.4 应用接入

区块链专网的应用接入应符合以下要求：

a） 支持链外业务系统对智能合约的调用、查询和事件监听；

b） 提供通用、方便的应用接入方式。

9.5 应用升级

区块链专网的应用升级应符合以下要求：

a） 支持应用基本信息、智能合约、节点配置、接入配置等内容的更新；

b） 支持停服务升级和非停服务升级两种升级方式。

9.6 应用卸载

区块链专网的应用卸载应符合以下要求：

a） 应用卸载支持具备链上数据备份和导出等功能；

b） 支持应用发布者主动发起应用卸载操作和平台管理者或监管方发起应用卸载操作。

10 与外部节点的数据交换

10.1 数据交换

区块链专网应具备通过节点网关与外部节点通信的能力，以及对外部节点运行状态数据进行监控的能力。

10.2 身份管理

区块链专网应为外部节点颁发唯一的节点身份证书。

10.3 通信安全

区块链专网内的应用应在通过安全的授权许可后再进行外部节点数据交互。

10.4 权限管理

区块链专网应具备支持外部节点加入、退出、禁用以及权限管理的能力。

11 运行维护

11.1 底层框架管理

区块链专网底层框架管理应符合以下要求：

a） 具备对专网内可用底层框架进行统一管理的能力；

b） 具备动态增加新联盟链底层框架的能力；

c） 具备查看专网内已适配底层框架的名称、版本号等基础信息的能力；

d） 具备对已适配底层框架运行状态进行统计分析的能力。

11.2 节点网关管理

节点网关管理内容应包括但不限于负载均衡、权限证书等。

11.3 系统运行监控

应具备对专网内节点运行状态、应用运行状态进行监控的能力，运行状态信息包括但不限于节点数量、应用数量、交易数量、块高等。

11.4 备份与恢复

区块链专网的备份与恢复应符合以下要求：

a） 具备对专网内数据进行备份与恢复的能力，备份内容包括但不限于账本数据、证书、密钥、操作系统日志、服务器配置等；

b） 具备在规定时限内进行故障恢复的能力，规定时限以实际需要为准。

11.5 应急预案管理

区块链专网应具备应急预案和针对应急预案的管理措施，并定期进行维护和优化。

12 安全体系

12.1 底层框架节点身份

区块链专网安全体系的底层框架节点身份应符合以下要求：

a） 专网由授权机构在节点加入系统前给予其在系统内唯一的身份标识，并提供与之对应的标识鉴别信息和标识凭证，授权机构应在凭证中指定节点角色；

b） 具有节点标识认证失败时的处理机制，采取结束通信、限制认证失败次数和超时自动结束等措施；

c） 应用PKI/CA系统进行强身份认证，实现统一身份认证和统一授权。

12.2 底层框架通信安全

区块链专网安全体系的底层框架通信安全应符合以下要求：

a） 采用密码技术保证底层框架通信过程中敏感信息字段或整个报文的保密性，应确保信息在存储、传输过程中不被非授权用户读取和篡改；

b） 跨区块链应用通信时，采用中继链模式，链应用之间交换信息通过中继链加密传输；

c） 采用有权限的网络访问控制，在参与专网底层框架间构建VPN；

d） 底层框架间通信协议应具备应对通信延时、中断等情况的处理机制。

12.3 网关通信安全

区块链专网安全体系应包含网关通信安全，且应符合以下要求：

a） 网关配置权限访问控制，防止来自内网、局域网、互联网或第三方网络的未授权用户或数据流量访问入侵；

b） 网关具备攻击检测能力，包括但不限于DoS攻击，以及其他安全威胁。

12.4 应用接入身份

区块链专网安全体系应包含应用接入身份管理，且应符合以下要求：

a） 具备对区块链应用接入的身份鉴权和授权能力，实现可审计、可追溯；

b） 应用的接入权限具备双重认证机制，包括CA身份认证及节点网关鉴权机制。

12.5 应用权限管理

区块链专网安全体系应包含应用权限管理，且应符合以下要求：

a） 具备对专网内不同联盟链底层框架下各应用的权限管理机制，建立专用的权限管理链，所有的区块链应用权限由权限管理链统一管理；

b） 对应用的每一次权限操作写入日志，尤其是敏感信息的查看和使用，用于复查和审计；

c） 提供基于区块链应用智能合约的权限管理，能够实现基于智能合约方法级的权限分配和授权访问控制。

12.6 用户身份管理

区块链专网安全体系应包含用户身份管理，且应符合以下要求：

a） 实现有效的用户身份管理，包括但不限于身份注册、身份核实、账户管理、身份更新和撤销等；

b） 用户身份信息变更或删除时，进行日志记录。

13 监管机制

13.1 监管内容

区块链专网应对以下内容进行监管：

a） 应用的名称、描述、类型、所涉及业务的合规性等；

b） 智能合约的类型、用途、数据模型及接口功能等。

13.2 监管方式

区块链专网的监管应符合以下要求：

a） 支持信息报备、穿透式监管、链外监管等多种监管方式；

b） 支持通过系统对接或线下方式，向监管机构或专网管理单位报备应用信息、智能合约、交易数据等；

c） 支持监管机构作为应用参与方进行穿透式监管，通过参与交易背书进行监管；

d） 支持监管机构以监管节点的方式对应用进行监管；

e） 支持将应用数据导出到监管机构或专网管理单位本地监管系统，进行人工或自动化智能监管。

参 考 文 献

[1] GB/T 25069-2010 信息安全技术 术语
[2] GB/T 37092-2018 信息安全技术 密码模块安全要求
[3] GM/T 0006-2012 密码应用标识规范
[4] GM/T 0009-2012 SM2密码算法使用规范
[5] GM/T 0010-2012 SM2密码算法加密签名消息语法规范
[6] GM/T 0015-2012 基于SM2密码算法的数字证书格式规范
[7] GM/T 0028-2014 密码模块安全技术要求
[8] GM/T 0039-2015 密码模块安全检测要求
[9] GM/T 0111-2021区块链密码应用技术要求
[10] GM/T 0115-2021 信息系统密码应用测评要求
[11] JR/T 0184-2020 金融分布式账本技术安全规范