ICS 35.240
CCS L 70

中华人民共和国国家标准

GB/T 42752—2023

区块链和分布式记账技术　参考架构

Blockchain and distributed ledger technology—Reference architecture

2023-05-23 发布　　2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　参考架构 …… 2
5.1　概述 …… 2
5.2　区块链用户视图 …… 2
5.3　区块链功能视图 …… 3
6　用户视图 …… 4
6.1　架构 …… 4
6.2　终端用户 …… 5
6.3　业务提供方 …… 5
6.4　技术提供方 …… 6
6.5　审计方 …… 7
6.6　治理方 …… 8
7　功能视图 …… 8
7.1　架构 …… 8
7.2　用户层 …… 8
7.3　服务接口层 …… 9
7.4　核心功能层 …… 10
7.5　基础设施层 …… 11
7.6　跨功能层 …… 11
参考文献 …… 14

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。

本文件由全国区块链和分布式记账技术标准化技术委员会(SAC/TC 590)提出并归口。

本文件起草单位：中国电子技术标准化研究院、中国人民银行数字货币研究所、上海万向区块链股份公司、深圳前海微众银行股份有限公司、中国平安保险(集团)股份有限公司、众安信息技术服务有限公司、厦门安妮股份有限公司、易见供应链管理股份有限公司、北京百度网讯科技有限公司、杭州趣链科技有限公司、深圳市腾讯计算机系统有限公司、蚂蚁区块链科技(上海)有限公司、江苏恒为信息科技有限公司、华为技术有限公司、智度科技股份有限公司、上海分布信息科技有限公司北京分公司、京东科技信息技术有限公司、深圳华大智造科技股份有限公司、四川长虹电子控股集团有限公司、浙商银行股份有限公司、国网区块链科技(北京)有限公司、福建省海峡区块链研究院、上海金丘信息科技有限公司、链极智能科技(上海)有限公司、复旦大学、深圳赛西信息技术有限公司、浙江大学、深圳区块大陆科技有限公司、敏于行(北京)科技有限公司、浙江泰科数联信息技术有限公司、中国工商银行股份有限公司、上海计算机软件技术开发中心、国信优易数据股份有限公司、北京好扑信息科技有限公司、上海奥若拉信息科技集团有限公司、北京众享比特科技有限公司、恒银金融科技股份有限公司、北京华标伟业科技发展有限公司、北京爱蜂科技有限公司、深圳市赛肯威科技有限公司、南京大学、智牛互联链金融科技(平潭)有限公司、迅鳐成都科技有限公司、电子科技大学。

本文件主要起草人：周平、穆长春、李鸣、于秀明、狄刚、杜宇、李斌、苏威硕、苏振彪、郝汉、刘天成、肖伟、李伟、武杨、张辉、李佳秾、郝玉琨、张开翔、蔡亮、张亮亮、崔春生、梁朋举、周炎、崔静、王义、王晨辉、徐磊、杨梦、唐博、臧铖、职亮亮、孙琳、高林挥、韩根、庞引明、阚海斌、刘朝伟、戴炳荣、宋文鹏、杨扬、刘洋、王春涛、马昊伯、毛新强、江浩然、李庆华、吕雪、晏海水、莫冰、李瑞、颜嘉麒、夏琦、高建彬、张雁。

区块链和分布式记账技术　参考架构

1　范围

本文件给出了区块链参考架构，规定了区块链参考架构涉及的用户视图和功能视图。

本文件适用于使用区块链和分布式记账技术的组织建设区块链系统；指导使用区块链和分布式记账技术的服务提供组织提供区块链服务；使用区块链和分布式记账技术的组织选择和使用区块链服务。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

活动　activity

一组特定任务的集合。

[来源：GB/T 32399—2015，3.2.1]

3.2

数字签名　digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人（例如接收者）伪造的目的。

[来源：GB/T 25069—2022，3.576]

3.3

功能组件　functional component

参与活动所需的、可实现的一个功能性基本构件块。

[来源：GB/T 32399—2015，3.2.3，有修改]

3.4

对等网络　peer-to-peer network

一种仅包含对控制和操作能力等效的节点的计算机网络。

[来源：GB/T 5271.18—2008，18.04.05]

3.5

事务　transaction

工作过程的最小单元，是产生符合规则要求的结果所需的一个或多个动作序列。

[来源：ISO 22739：2020，3.77]

3.6

区块　block

一种包含区块链元数据和交易数据的数据结构。

注：区块是组成区块链的基本结构单元。

3.7

共识　consensus

在分布式节点间达成区块数据一致性认可的结果。

3.8

共识机制　consensus mechanism

在分布式节点间达成共识(3.7)的规则和程序。

3.9

账本　ledger

按照时序方法组织的事务(3.5)数据集合。

3.10

分布式账本　distributed ledger

在分布式节点间共享并使用共识机制(3.8)实现具备一致性的账本。

3.11

分布式记账技术　distributed ledger technology

实现分布式账本(3.10)的技术的集合。

3.12

区块链　blockchain

使用密码技术链接将共识确认过的区块(3.6)按顺序追加形成的分布式账本(3.10)。

3.13

智能合约　smart contract

存储在分布式账本(3.10)中的计算机程序。

注：智能合约的共识执行结果都记录在分布式账本中。

4　缩略语

下列缩略语适用于本文件。

BRA：区块链参考架构(Blockchain Reference Architecture)

IDE：集成开发环境(Integrated Development Environment)

SLA：服务级别协议(Service Level Agreement)

5　参考架构

5.1　概述

BRA 采用视图方法对区块链系统进行描述，包括用户视图和功能视图。

5.2　区块链用户视图

5.2.1　概述

用户视图实体包括区块链系统相关方、共同关注点、角色、子角色和活动。用户视图实体见图 1。

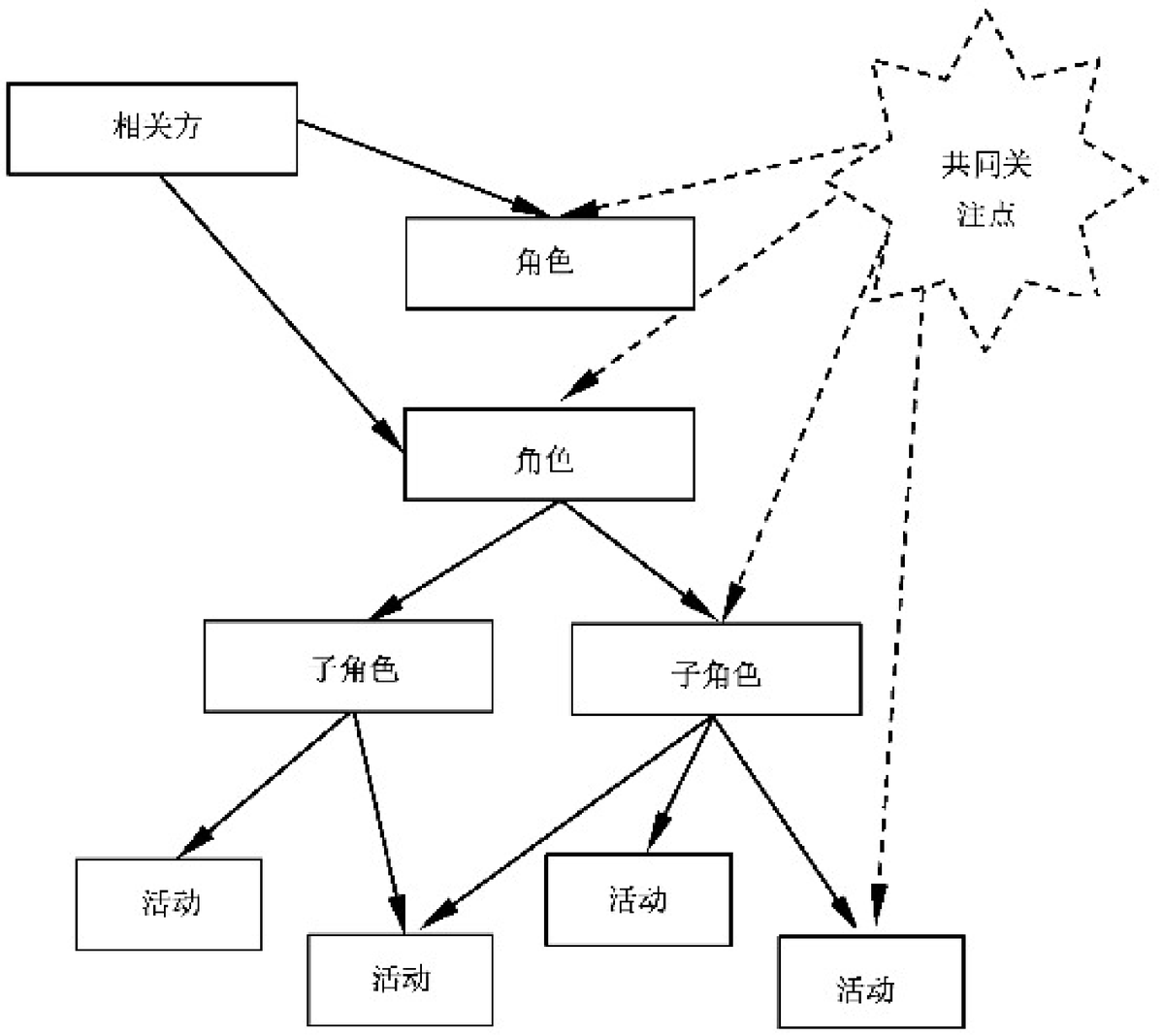

图 1　用户视图实体

5.2.2　相关方

相关方是区块链系统的利益相关者。在某个给定时间点，一个相关方可承担多个角色。

5.2.3　共同关注点

共同关注点是在不同角色之间协调，且在区块链系统中一致实现的行为或能力，适用于多个不同角色或功能组件。共同关注点能被多个角色、子角色和活动共享。

5.2.4　角色

角色是一组服务于共同目的活动的集合。

5.2.5　子角色

子角色是特定角色的所有活动的子集。某个角色的区块链活动能被该角色下的不同子角色所共享。

5.2.6　活动

活动是一组特定区块链任务的集合，需要有目标，并能交付一个或多个结果。

5.3　区块链功能视图

5.3.1　概述

功能视图是构建区块链系统所需功能的技术中立视图，描述了支持区块链活动所需的功能。功能视图中功能层、跨功能层和功能组件之间的相互关系见图 2。

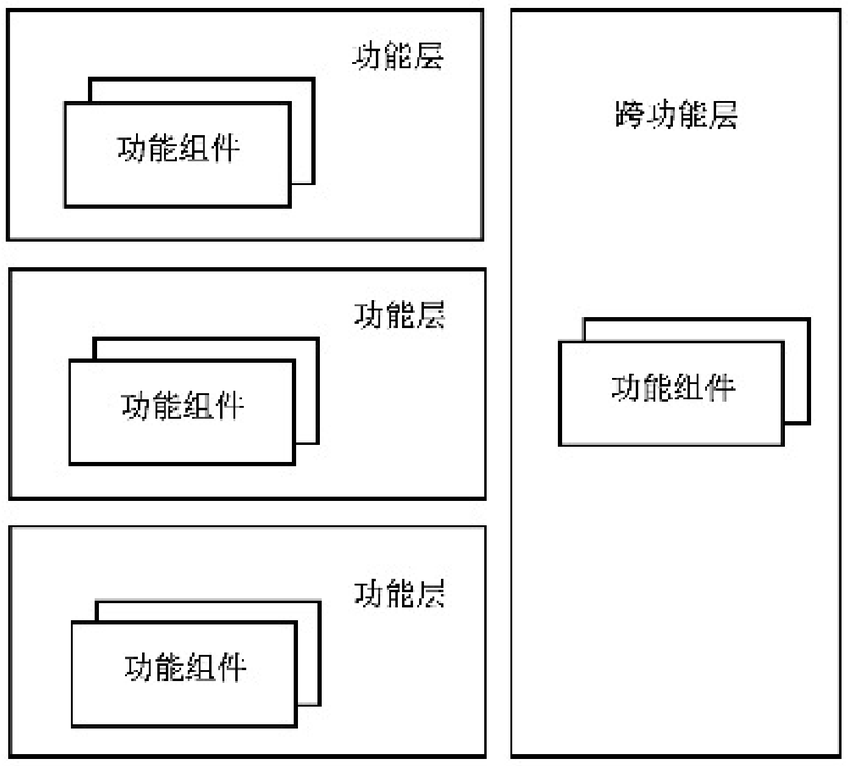

图 2　功能层、跨功能层和功能组件的关系

5.3.2　功能层

功能层是一组提供类似功能或服务于共同目标的功能组件的集合。

5.3.3　跨功能层

跨功能层是提供跨越多个功能层的功能组件的集合。

5.3.4　功能组件

功能组件是参与某一活动所需的，且能实现功能的组件。

6　用户视图

6.1　架构

区块链系统用户视图包括终端用户、业务提供方、技术提供方、审计方和治理方。区块链系统用户视图架构见图 3。

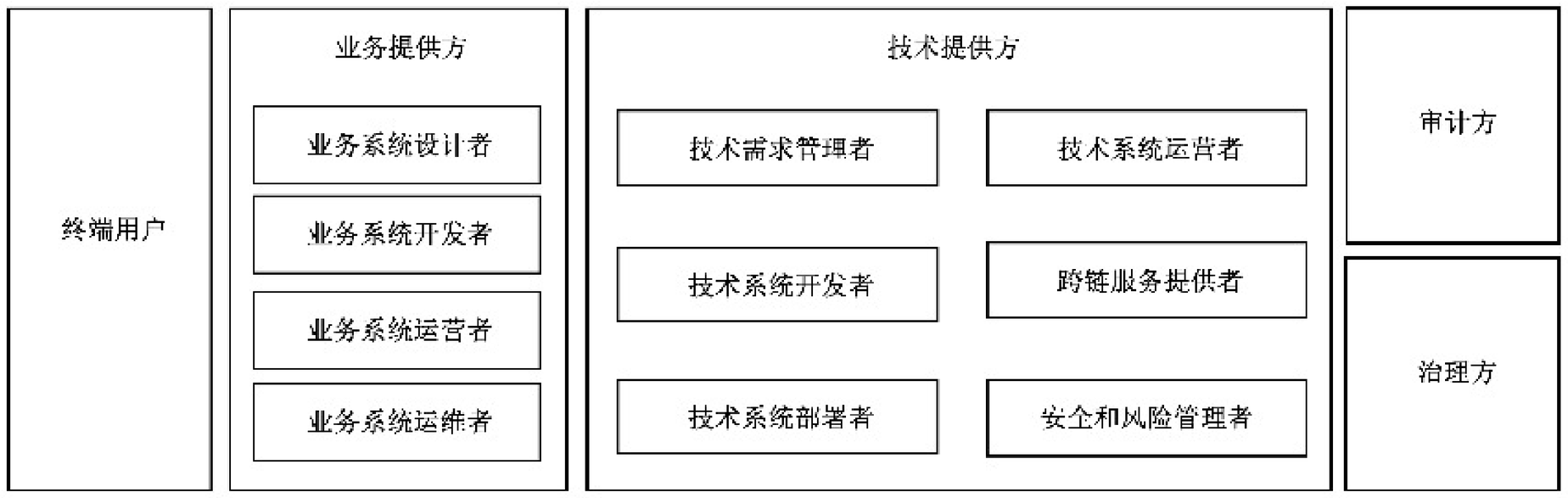

图 3　区块链系统用户视图架构

6.2 终端用户

终端用户是区块链服务的最终使用方，通过使用业务提供方的服务或应用实现业务需求。使用区块链活动的方式宜包括：

a） 通过客户端或用户图形接口使用区块链服务；

b） 通过命令行界面使用区块链服务；

c） 通过执行脚本使用区块链服务。

6.3 业务提供方

6.3.1 相关活动

业务提供方包括业务系统设计者、业务系统开发者、业务系统运营者和业务系统运维者。业务提供方相关的区块链活动见图 4。

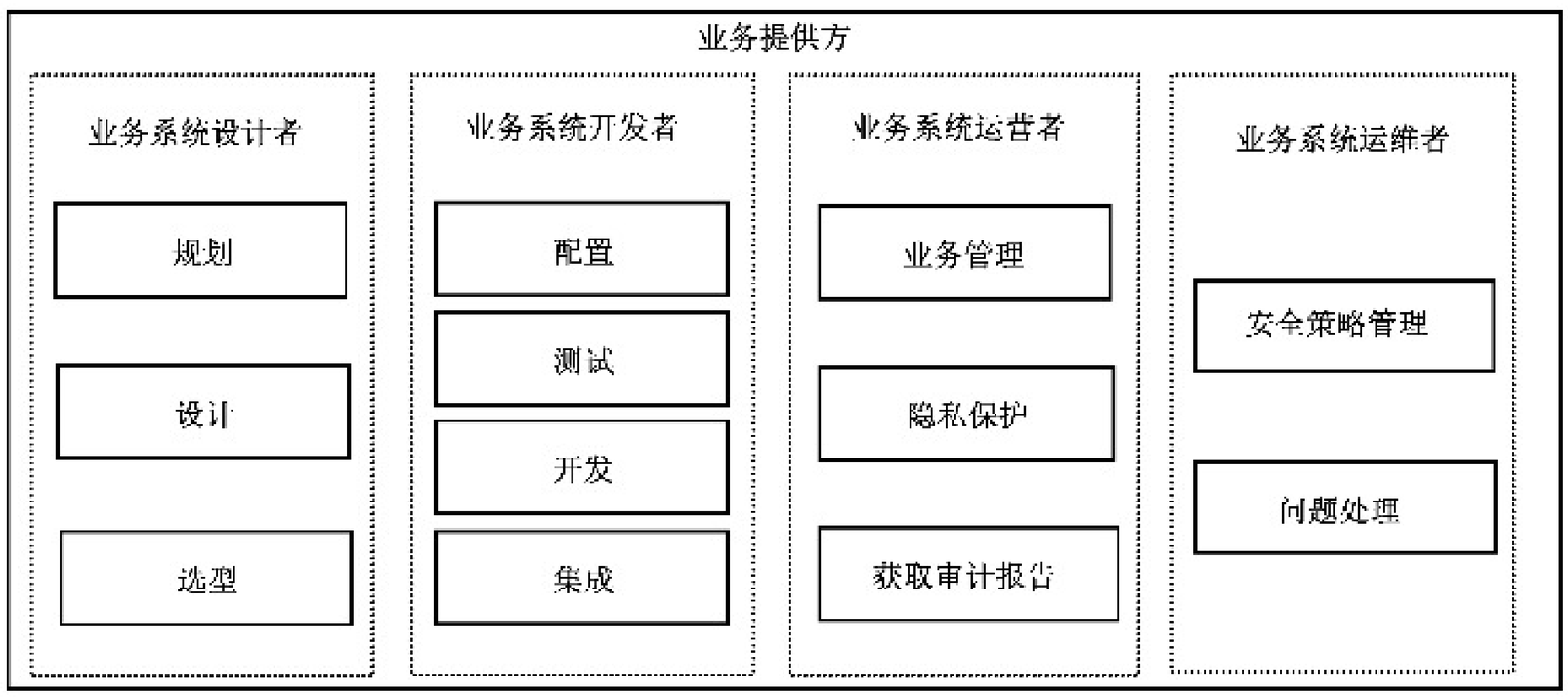

图 4 业务提供方相关的区块链活动

6.3.2 业务系统设计者

业务系统设计者是业务提供方的子角色。其活动应包括：

a） 规划：根据业务需求，制定系统既定的业务目标；

b） 设计：根据业务规划，设计业务系统与区块链的关系，明确所需的相关系统及集成方式；

c） 选型：根据业务设计和关键问题，选择区块链服务。

6.3.3 业务系统开发者

业务系统开发者是业务提供方的子角色。其活动应包括：

a） 配置：对选定业务系统的权限和账户等进行配置；

b） 测试：对选定业务系统的功能和性能等进行测试；

c） 开发：对业务系统的功能组件和接口进行开发；

d） 集成：对业务系统与其他业务系统进行集成。

6.3.4 业务系统运营者

业务系统运营者是业务提供方的子角色。其活动应包括：

a） 业务管理：管理业务系统，包括但不限于工作流管理和用户管理等；

b) 隐私保护:制定和执行隐私保护策略;

c) 获取审计报告。

6.3.5 业务系统运维者

业务系统运维者是业务提供方的子角色。其活动应包括:

a) 安全策略管理;

b) 问题处理。

6.4 技术提供方

6.4.1 相关活动

技术提供方包括技术需求管理者、技术系统开发者、技术系统部署者、技术系统运营者、跨链服务提供者、安全和风险管理者。技术提供方相关的区块链活动见图 5。

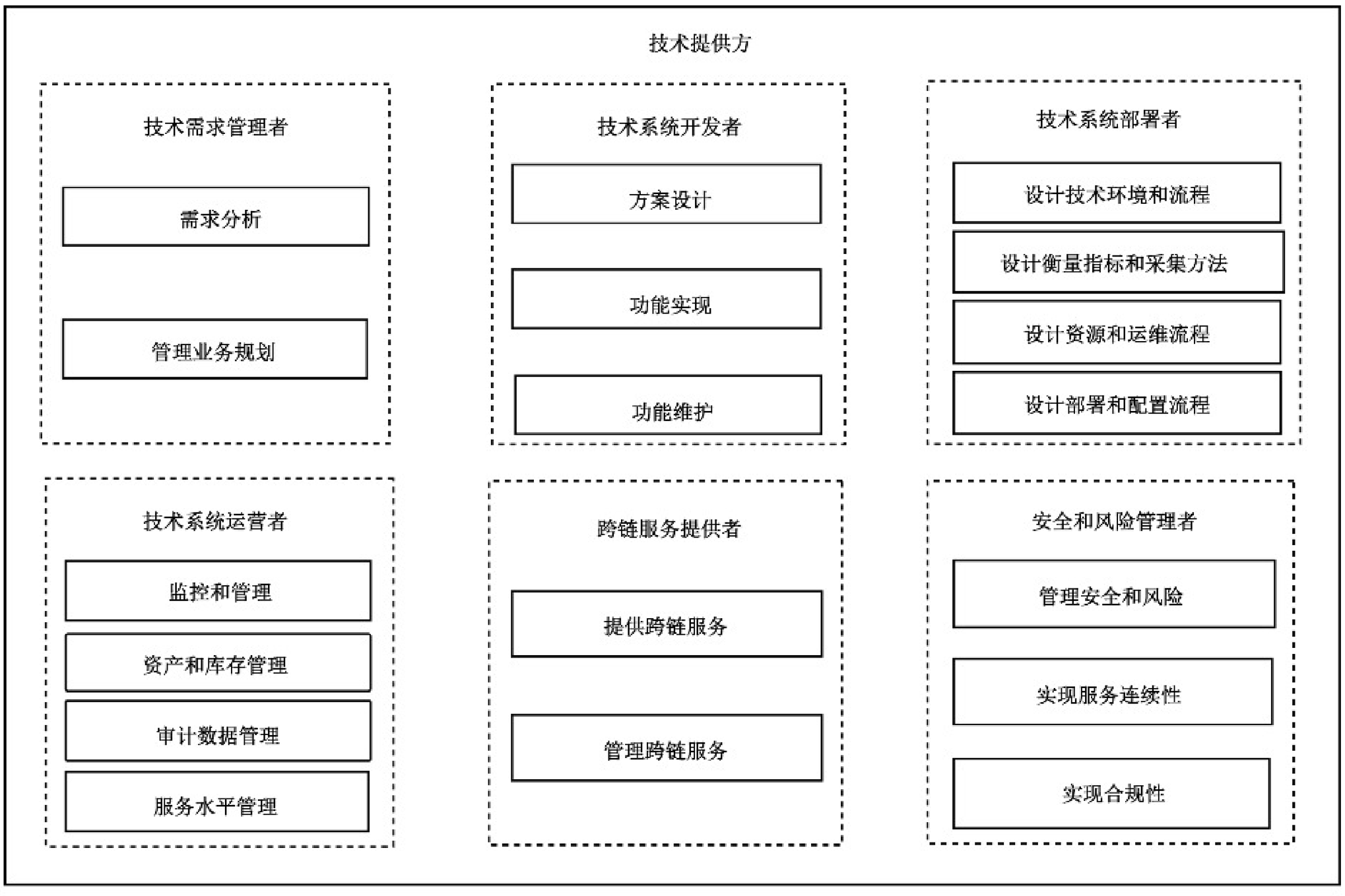

图 5 技术提供方相关的区块链活动

6.4.2 技术需求管理者

技术需求管理者是技术提供方的子角色。其活动应包括:

a) 需求分析:响应业务提供方的服务请求,收集和管理业务提供方的业务和技术需求,改进区块链系统;

b) 管理业务规划:协调技术提供方与业务提供方之间的关系。

6.4.3 技术系统开发者

技术系统开发者是技术提供方的子角色。其活动应包括：

a) 方案设计：根据需求，分析和设计业务提供方所需的区块链系统；

b) 功能实现：开发完整的和可交付的区块链系统；

c) 功能维护：根据业务提供方的业务需求、技术需求和异常情况，维护和更新区块链系统。

6.4.4 技术系统部署者

技术系统部署者是技术提供方的子角色。其活动应包括：

a) 设计技术环境和流程：设计系统运行所需的技术环境和操作流程；

b) 设计衡量指标和采集方法：设计系统的衡量指标及采集方法；

c) 设计资源和运维流程：设计系统运行过程所依赖的资源和可用的运维流程；

d) 设计部署和配置流程：设计系统的部署和配置流程。

6.4.5 技术系统运营者

技术系统运营者是技术提供方的子角色。其活动应包括：

a) 监控和管理：监控和管理系统及相关基础设施运行情况；

b) 资产和库存管理：更新、运行和处置计算、存储、网络和软件等资源；

c) 审计数据管理：收集和提供审计相关数据；

d) 服务水平管理：管理服务与 SLA 之间的符合性。

6.4.6 跨链服务提供者

跨链服务提供者是技术提供方的子角色。其活动应包括：

a) 提供跨链服务：通过技术平台等为跨链服务提供支撑；

b) 管理跨链服务：通过配置资源、权限和安全措施等为跨链服务提供支撑。

6.4.7 安全和风险管理者

安全和风险管理者是技术提供方的子角色。其活动应包括：

a) 管理安全和风险：实现业务提供方和技术提供方信息安全策略的一致性，符合 SLA 中的安全要求；

b) 实现服务连续性：通过故障转移和冗余等方法，符合 SLA 中的服务要求；

c) 实现合规性：实现对法规和标准合规性的支持。

6.5 审计方

审计方通过监督、评价和咨询等方式，落实区块链相关的法律法规、监管规则和治理要求。其活动应包括：

a) 审计区块链系统治理的健全性和有效性；

b) 审计区块链服务的合规性和有效性；

c) 审计区块链系统内部控制的适当性和有效性；

d) 审计区块链系统风险管理的全面性和有效性；

e) 审计区块链账本记录的完整性和准确性；

f) 审计区块链系统的持续性、可靠性和安全性；

g) 审计其他事项。

6.6 治理方

治理方协调和管理终端用户、业务提供方、技术提供方和审计方的相互关系。其活动应包括：

a) 建立区块链组织架构，明确区块链系统内各相关主体的职责边界；

b) 建立区块链系统的管控、激励和约束机制；

c) 建立区块链系统的冲突管理和信息披露管理机制；

d) 完善区块链系统风险管理与内部控制；

e) 通过决策、执行和监督机制实现区块链服务的合法合规。

7 功能视图

7.1 架构

区块链系统功能视图包括用户层、服务接口层、核心功能层、基础设施层和跨功能层，内容如下：

a) 用户层执行与用户相关区块链服务的管理、维护和使用；

b) 服务接口层提供区块链访问和监控支持；

c) 核心功能层基于基础设施层实现相应功能，并为服务接口层提供相关支持；

d) 基础设施层提供区块链系统正常运行所需的环境和基础组件；

e) 跨功能层提供跨越用户层、服务接口层、核心功能层和基础设施层的功能组件。

区块链系统功能视图架构见图 6。

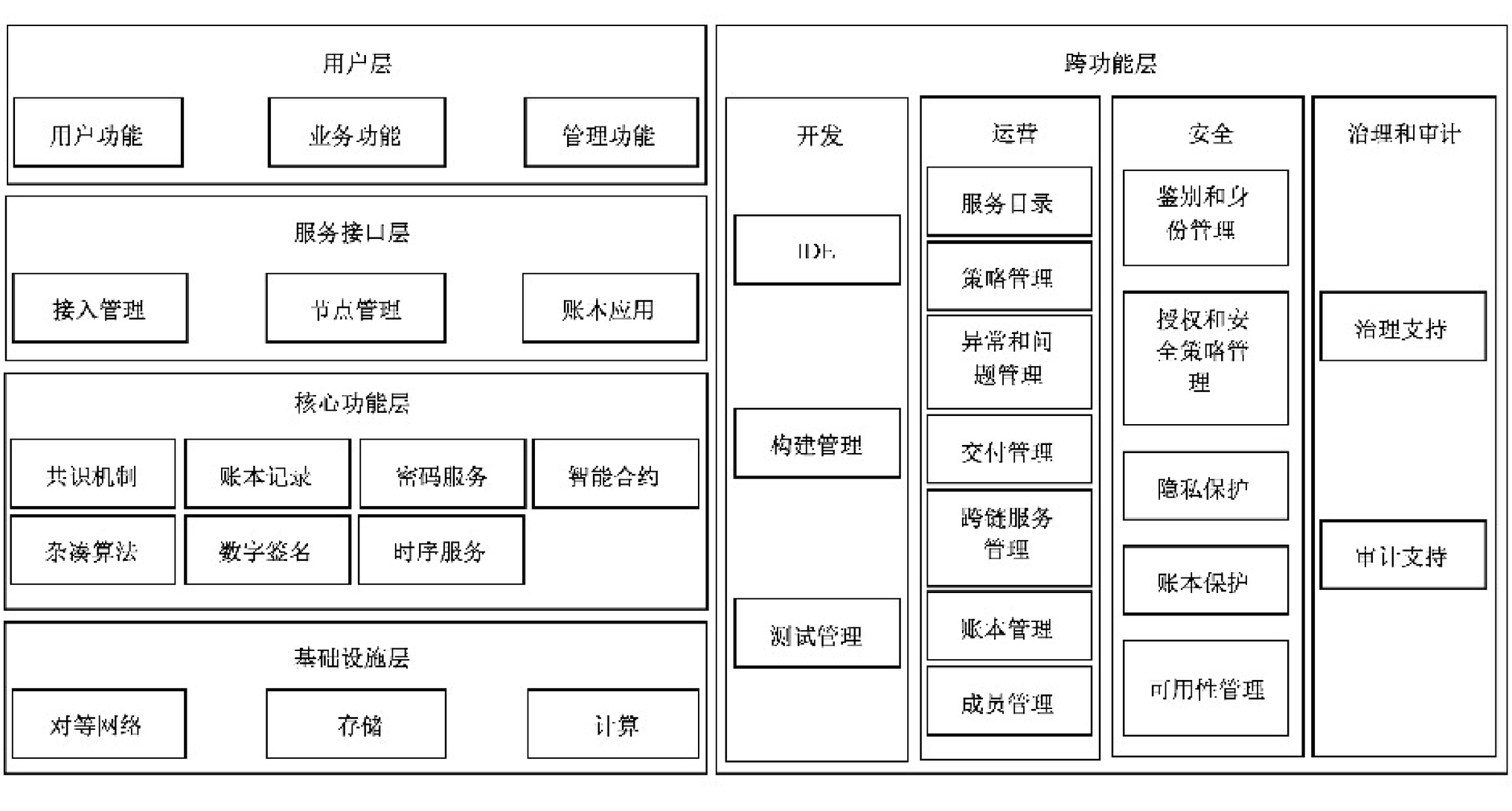

图 6 区块链系统功能视图架构

7.2 用户层

7.2.1 用户功能

用户功能功能组件支持终端用户访问和使用区块链服务。其功能应包括：

a) 提供用户界面：可采用命令行界面、图形用户接口或应用编程接口等形式；
b) 提交事务请求：将终端用户的查询、交易和合约操作等特定事务请求提交到区块链网络。

7.2.2 业务功能

业务功能功能组件支持业务提供方、技术提供方、审计方和治理方的活动。其功能应包括：
a) 业务管理：对业务相关权限、流程和数据进行管理；
b) 服务集成：根据不同业务需求，有选择性地集成数据交换和跨链等服务；
c) 技术服务支持：根据业务需求和规划，支持业务系统的开发、运维和安全保障；
d) 治理和审计：为区块链业务服务提供合规治理和审计等服务。

7.2.3 管理功能

管理功能功能组件支持对区块链用户的管理。其功能应包括：
a) 事件管理：提供预定义或自定义事件的服务；
b) 问题管理：提供区块链业务与跟踪和报告系统问题的服务；
c) 安全管理：提供账户、事件和合约安全的服务；
d) 监控管理：提供系统故障和运行状态监控的服务。

7.3 服务接口层

7.3.1 接入管理

接入管理功能组件提供跨进程调用功能，为用户层和核心功能层提供接入服务。其功能应包括：
a) 账户信息查询：提供区块链用户账户体系相关的基本信息查询服务；
b) 账本信息查询：提供区块和事务详情等查询服务；
c) 事务操作处理：将区块链用户提交的特定事务操作请求提交到区块链网络；
d) 外部数据接入：提供区块链外部可信数据源的安全接入能力；
e) 接口服务能力管理：支持接口调用频度、事务操作和账本查询缓存设置；
f) 接口访问权限管理：针对不同用户配置不同等级的访问权限。

7.3.2 节点管理

节点管理功能组件支持对区块链节点的信息查询、管理和控制。其功能应包括：
a) 信息查询：提供区块链节点服务器的状态信息查询服务；
b) 启动关闭控制：提供区块链节点服务器的启动与关闭服务；
c) 服务配置：提供区块链节点服务器的节点服务能力配置；
d) 网络状态监控：提供区块链节点服务器网络连接状态监控服务；
e) 授权管理：提供区块链节点准入准出配置、节点事务处理和账本查询授权配置。

7.3.3 账本应用

账本应用功能组件通过调用核心功能层功能组件，实现基于区块链账本记录功能组件的应用。其功能应包括：
a) 支持链上内容发布；
b) 对特定事务进行多签名权限控制设置；
c) 基于智能合约功能组件执行合约逻辑。

7.4 核心功能层

7.4.1 共识机制

共识机制功能组件通过特定的共识算法，完成区块链网络节点的共识过程。其功能应包括：

a) 支持多个节点参与共识和验证；

b) 支持独立节点对区块链网络提交的相关信息进行有效性验证；

c) 支持识别并拒绝未经共识确认的新增或修改信息；

d) 具备一定的容错性，包括物理或网络故障等非恶意错误、节点遭受非法控制等恶意错误和节点产生不确定行为等不可控错误等。

7.4.2 账本记录

账本记录功能组件实现区块链中分布式数据的存储。其功能应包括：

a) 支持账本数据的持久化存储；

b) 支持多节点拥有延时完整数据；

c) 支持向节点提供已授权数据。

7.4.3 密码服务

密码服务功能组件应经过国家密码管理部门认证或核准使用。其功能应包括：

a) 支持 SM2、SM3、SM4 和 SM9 等商密算法；

b) 具备明确的密钥管理方案，实现区块链底层安全机制的正常运行。

7.4.4 智能合约

智能合约功能组件支持在预设规则前提下，根据特定输入产生特定结果。其功能应包括下列内容。

a) 开发运行环境，包括：

1) 提供编程语言支持，必要时提供配套的 IDE；

2) 支持合约内容静态和动态检查；

3) 提供运行载体支持，如虚拟机等；

4) 对于与区块链系统外部数据进行交互的智能合约，外部数据源的影响范围应仅限于智能合约范围内，不应影响区块链系统的整体运行。

b) 开发存储环境，包括：

1) 防止对合约内容进行篡改；

2) 支持多方共识下的合约升级；

3) 支持向账本中写入合约内容。

7.4.5 杂凑算法

杂凑算法功能组件应具有以下特征：

a) 不可预测性：已知输入值的情况下，函数值不可预测；

b) 不可逆性：已知函数值的情况下，恢复函数输入的难度不小于破译密码服务中加密算法的难度；

c) 可验证性：同样输入必然得到同样输出，且函数值的正确性可被独立验证；

d) 具备抗撞击能力：不同输入得出同样输出的概率极小。

7.4.6 数字签名

数字签名功能组件包括签名和验签。签名指签名者用私钥对信息原文进行处理生成数字签名值。

验签指验证者利用签名者公开的公钥对签名值和信息原文验证签名。数字签名功能应包括：

a） 采用7.4.3中给出的数字签名算法；

b） 在部分应用场景下，具有权威公正的第三方签发的数字证书。

7.4.7 时序服务

时序服务功能组件通过选择特定的时序机制或工具，保障区块链系统行为或数据记录的一致性。其功能应包括：

a） 支持统一账本记录时序；

b） 具备时序容错性。

7.5 基础设施层

7.5.1 对等网络

区块链系统采用分布式对等网络协议组织区块链中的各网络节点。其功能应包括：

a） 提供点对点的高效安全通信；

b） 提供点对点通信基础上的多播能力。

7.5.2 存储

存储功能组件实现区块链运行过程中产生各类数据的存储。其功能包括通过数据的分布式存储提高数据可靠性等。

7.5.3 计算

计算功能组件提供区块链系统运行的计算能力。其功能应包括：

a） 对区块链系统提供运行支持；

b） 能够被对等网络中的每个节点采用。

7.6 跨功能层

7.6.1 开发

7.6.1.1 IDE

IDE功能组件用于提供智能合约、分布式记账技术及相关应用的开发、调试和部署等服务组合工具。其功能应包括：

a） 支持使用服务的核心功能层和访问服务的基础设施层；

b） 支持生成开发服务相关的配置数据；

c） 支持服务配置脚本和组件的编写或生成。

7.6.1.2 构建管理

构建管理功能组件用来构建可发布的软件包。其功能应包括：

a） 支持自动化构建软件包功能；

b） 提供自动化编译功能；

c） 在构建过程出错时，提供出错信息；

d） 实现构建过程的审核。

7.6.1.3 测试管理

测试管理功能组件支持对区块链服务进行测试。其功能包括：

a) 应支持对测试计划、测试方案、测试报告和测试用例等管理；

b) 应支持自动生成测试报告；

c) 应具备测试用例库和测试数据库管理等功能；

d) 宜支持自动化测试。

7.6.2 运营

7.6.2.1 服务目录

服务目录功能组件提供区块链服务提供方的服务列表。服务列表应包括提供、部署和运行区块链服务有关的信息。

7.6.2.2 策略管理

策略管理功能组件应提供区块链服务的定义、更新和访问策略及针对这些策略的管理。

7.6.2.3 异常和问题管理

异常和问题管理功能组件应提供异常和问题的发现和报告能力，并通过分析和处置流程解决异常问题。

7.6.2.4 交付管理

交付管理功能组件通过系统实现或访问终端等方式，提供区块链系统服务交付功能。交付管理应设置必要的工作流程，实现相关交付单元按时、按序和按量交付。

7.6.2.5 跨链服务管理

跨链服务管理功能组件应根据请求建立区块链服务提供者与跨链服务提供者间的联系，并支持交换双方的身份和鉴别等信息。

7.6.2.6 账本管理

账本管理功能组件应提供维护和监督账本所有权和活动的功能。

7.6.2.7 成员管理

成员管理功能组件用于管理区块链系统成员的行为。其功能应包括：

a) 管理与确定成员身份；

b) 保护系统成员的个人隐私信息；

c) 设置机密数据的访问权限；

d) 支持数据审计。

7.6.3 安全

7.6.3.1 鉴别和身份管理

鉴别和身份管理功能组件用于确认用户身份。其功能应包括：

a) 支持确认用户对特定资源的访问和使用权限；

b） 支持建立身份管理策略；
c） 支持利用身份鉴别方法支撑身份管理策略；
d） 支持在身份鉴别的基础上，建立用户身份管理机制。

7.6.3.2 授权和安全策略管理

授权和安全策略管理功能组件用于权限和安全策略的管理。其功能应包括：
a） 授予用户访问和使用资源的权限；
b） 设置授权和安全规则。

7.6.3.3 隐私保护

隐私保护功能组件用于保护敏感信息不被泄露或非法使用。其功能应包括：
a） 支持获得授权机构在区块链上代理用户进行事务处理；
b） 支持将数据传输限制在特定授权节点间；
c） 支持对用户数据访问权限进行控制；
d） 支持对事务发起方和接收方的信息及事务信息本身进行隐私保护。

7.6.3.4 账本保护

账本保护功能组件用于对账本的事务信息提供隐私保护。其功能应包括：
a） 建立账本访问控制机制；
b） 支持账本记录和日志备份；
c） 提供具有安全隔离能力的账本存储环境；
d） 对账本提供正确性、一致性和完整性验证。

7.6.3.5 可用性管理

可用性管理功能组件实现区块链系统基本功能和服务的可用，应支持容量管理、配置管理、可靠性管理、记录和监控等工具。

7.6.4 治理和审计

7.6.4.1 治理支持

治理支持功能组件用于支持区块链系统符合治理机构对于区块链服务的要求。其功能包括：
a） 应建立治理体系，并通过事前准入控制、事中权限控制和事后追溯等技术手段实现治理目标；
b） 应设置明确的治理规则，并宜通过自动化方式实现；
c） 应收集、记录和保存治理活动相关的日志和记录等数据；
d） 宜支持加入治理节点，并宜对数据完整性、有效性和流程合规性进行实时监督与干预；
e） 宜支持利用智能合约等技术执行治理活动。

7.6.4.2 审计支持

审计支持功能组件用于实现责任鉴定和事件追溯等方面的要求。其功能包括：
a） 应保存与审计活动相关的数据和证据；
b） 宜支持对区块链活动的事前、事中和事后三阶段进行审计；
c） 宜支持加入审计节点；
d） 宜支持区块链网络与审计系统间的联系。

参 考 文 献

[1] GB/T 5271.18—2008 信息技术 词汇 第18部分:分布式数据处理

[2] GB/T 11457—2006 信息技术 软件工程术语

[3] GB/T 25069—2022 信息安全技术 术语

[4] GB/T 32399—2015 信息技术 云计算 参考架构

[5] ISO/IEC 9804:1998 Information technology—Open Systems Interconnection—Service definition for the Commitment, Concurrency and Recovery service element

[6] ISO/IEC 17789:2014 Information technology—Cloud computing—Reference architecture

[7] ISO 22739:2020 Blockchain and distributed ledger technologies—Vocabulary

[8] ISO 23257:2022 Blockchain and distributed ledger technologies—Reference architecture

[9] ISO/IEC/IEEE 42010 Software, systems and enterprise—Architecture description