中国区块链技术和产业发展论坛标准

CBD-Forum-001-2017

区块链 参考架构

Blockchain—Reference Architecture

（发布稿）

2017-05-16 发布

目 录

前　言

区块链作为一种新兴的应用模式，在金融服务、供应链管理、文化娱乐、智能制造、社会公益和教育就业等领域有着广泛的应用价值。近几年来，区块链技术和应用正经历快速发展的过程。与此同时，国内国际上区块链领域的标准仍属空白，行业发展碎片化，行业应用存在一定的盲目性，不利于区块链的应用落地和技术发展。区块链的标准化有助于统一对区块链的认识，规范和指导区块链在各行业的应用，以及促进解决区块链的关键技术问题，对于区块链产业生态发展意义重大。目前，国内外标准化组织已将区块链标准化提上议事日程，开展了组织建设、标准预研等一系列工作，并初步取得了一定进展。

中国电子技术标准化研究院作为国际标准化组织ISO/TC 307（区块链和分布式账本技术技术委员会）的国内技术归口单位，在本标准研制过程中，充分发挥了组织协调和技术方向把关作用。标准研制的流程和标准参照国际标准和行业标准研制的相关规则和规定，标准工作组聚集了国内区块链行业多个领域的技术和管理专家，开展了多种形式的专题研讨、专家和企业征求意见活动，在保证标准专业性的同时，也确保了标准研制过程的公开性和透明性。此外，为了保证标准内容的科学性、合理性和可实施性，中国电子技术标准化研究院根据标准研制情况，组织开发了配套的测试验证方案，并对乐视链服信息技术（北京）有限公司、北京瑞卓喜投科技发展有限公司、上海分布信息科技有限公司、众安信息技术服务有限公司、杭州趣链科技有限公司等重点参与企业的区块链解决方案进行了测试验证。

本标准的研制工作，得到了中国区块链技术和产业发展论坛专家委员会的指导和支持，专家委员会主任、北京理工大学副校长梅宏院士，和各位专家成员，对标准内容和文稿进行了深入严谨的讨论，给出了许多切实有益的意见，对标准质量提升和标准内容完善起到关键性作用。除此之外，来自同济大学、复旦大学、浙江大学等高校和研究院所的知名学者，以及来自中国证监会、中国工商银行、中国农业银行、中国移动、中国外汇交易中心、邮储银行、中国人寿保险、深圳证券交易所等企事业单位的资深专家，从不同行业视角针对标准提出了诸多建设性意见，提高了标准的适用性和可实施性。在此对所有专家的指导和帮助表示由衷的谢意。

本标准负责起草单位：中国电子技术标准化研究院、上海万向区块链股份公司、浙江蚂蚁小微金融服务集团有限公司、深圳前海微众银行股份有限公司、乐视链服信息技术（北京）有限公司、万达网络科技集团有限公司、中国平安保险（集团）股份有限公司、上海金丘实业股份有限公司、上海钜真金融信息服务有限公司、鑫苑（中国）置业有限公司、众安信息技术服务有限公司、上海分布信息科技有限公司、用友网络科技股份有限公司、海航生态科技集团有限公司、三一集团有限公司。

本标准主要起草人：周平、唐晓丹、宋文鹏、谭智勇、李斌、季宙栋、李俊、李奕、陈家乐、吴小川、华正皓、陈志峰、李彦博、金龙、杜宇、赵峰、吴涛、韩梅、高林挥、杨宝刚、曾林钊、马环宇、张开翔、蔡承杰、李佳秾、郝玉琨、李鸣、高西林、杜君君、倪旻、易锋平、柴庆朋、丁阳、文博武、李升林。

使用帮助信息：任何单位和个人在使用本标准的过程中，若存在疑问，或有对本标准的改进建议和意见，请与中国电子技术标准化研究院（中国区块链技术和产业发展论坛 秘书处）联系。

电话：010-64102801/2804；电子邮件：cbdforum@cesi.cn

通信地址：北京东城区安定门东大街1号（100007）

为了推动本标准的持续改进，使其内容更加贴近用户组织的实际需求，欢迎社会各方力量参加本标准的持续改进，本标准的更多信息欢迎关注中国区块链技术和产业发展论坛官方网站和公众号。

http://www.cbdforum.cn

区块链 参考架构

1 范围

本标准规定了**区块链**参考架构（BRA）。具体规定了以下内容：

a） **区块链**参考架构涉及的用户视图、功能视图；

b） 用户视图所包含的**角色**、**子角色**及其**活动**，以及**角色**之间的关系；

c） 功能视图所包含的**功能组件**及其具体功能，以及**功能组件**之间的关系；

d） 用户视图和功能视图之间的关系。

本标准适用于：

a） 计划使用**区块链**和**分布式账本技术**的组织选择和使用**区块链**服务；

b） 计划使用**区块链**和**分布式账本技术**的组织建设**区块链**系统；

c） 指导使用**区块链**和**分布式账本技术**的服务提供组织提供**区块链**服务。

注：区块链和**分布式账本技术**的关系详见附录 A，二者具有共同点，又不能完全互换，在描述具体的系统时，通常采用“**区块链**”一词。

2 术语和缩略语

GB/T 25069-2010、GB/T 11457-2006、ISO/IEC 9804-1998、GB/T 5271.18-2008和GB/T 32399-2015界定的以下术语和定义适用于本文件。

2.1 其他标准中定义的术语

2.1.1

活动 activity

一组特定任务的集合。

[GB/T 32399-2015]

2.1.2

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

[GB/T 25069-2010]

2.1.3

分布式应用 distributed application

使用开放式系统互联环境中的两个或更多个应用实体调用来完成信息处理。

[ISO/IEC 9804:1998]

2.1.4

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。

[GB/T 25069-2010]

2.1.5

功能组件 functional component

参与**活动**（2.1.1）所需的，可实现的一个功能性基本构件块。

[GB/T 32399-2015]

2.1.6

互操作 interoperability

a） 两个或多个系统或组件交换信息并相互使用已交换的信息的能力；

b） 两个或两个以上系统可互相操作的能力。

[GB/T 11457-2006]

2.1.7

模块化 modularization

把系统分成若干模块（模块变成元素）以便于设计和开发。

[GB/T 11457-2006]

2.1.8

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。

[GB/T 5271.18-2008]

2.1.9

角色 role

一组服务于共同目的的**活动**（2.1.1）的集合。

[GB/T 32399-2015]

2.1.10

子角色 sub-role

特定角色（2.1.9）的所有**活动**的一个子集。

[GB/T 32399-2015]

2.2 本标准中定义的术语

2.2.1

区块链 blockchain

一种在**对等网络**（2.1.8）环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的**块链式数据结构**（2.2.2），实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

2.2.2

块链式数据结构 chained-block data structure

一段时间内发生的事务处理以区块为单位进行存储，并以密码学算法将区块按时间顺序连接成链条的一种数据结构。

2.2.3

共识算法 consensus algorithm

区块链系统中各节点间为达成一致采用的计算方法。

2.2.4

摘要算法 digest algorithm

又称摘要函数（或称 Hash 函数），通常通过将任意长度的消息输入变成固定长度的短消息输出来保障数据的完整性。

2.2.5

分布式账本 distributed ledger

可以在多个站点、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。

2.2.6

分布式账本技术 distributed ledger technology

实现分布式账本（2.2.5）的技术的集合。

2.2.7

智能合约 smart contract

以数字形式定义的能够自动执行条款的合约。

注：在**区块链**（2.2.1）技术领域，智能合约是指基于预定事件触发、不可篡改、自动执行的计算机程序。

2.3 缩略语

下列缩略语适用于本标准。

AES 高级加密标准（Advanced Encryption Standard）
API 应用编程接口（Application Programming Interface）
BRA 区块链 参考架构（Blockchain-Reference Architecture）
BSC 区块链服务客户（Blockchain Service Customer）
BSR 区块链服务关联方（Blockchain Service Related Party）
BSP 区块链服务提供方（Blockchain Service Provider）
DLT 分布式账本技术（Distributed Ledger Technology）
ECC 椭圆曲线加密（Elliptic Curve Cryptography）
IDE 集成开发环境（Integrated Development Environment）
SLA 服务水平协议（Service Level Agreement）

3 概述

3.1 本标准的约定

本标准采用以下约定：

a） 本标准使用一组图来帮助理解 BRA。图 1 给出了图中使用的图例。

注：图1中，“关注点”指的是共同关注点。

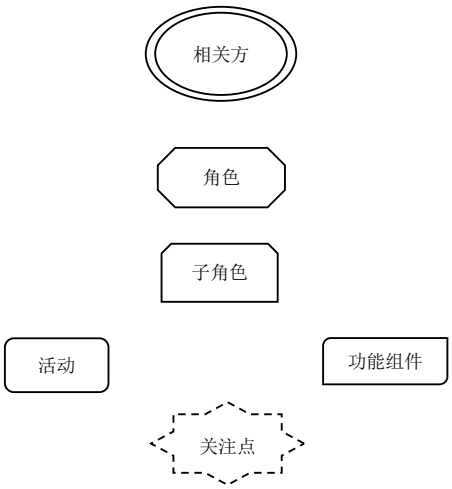


图1 本标准的图中使用的图例

b） 引用第二章中术语时用粗体字标识。

3.2 参考架构的作用

本标准中的 BRA 提供了一个体系框架，用于有效描述区块链**角色**、**子角色**、**区块链活动**、共同关注点、功能架构和**区块链功能组件**。

BRA 的作用包括：

- 描述**区块链**的利益相关者群体；
- 描述**区块链**系统的基本特征；
- 规范基本的**区块链活动**和**功能组件**，描述它们之间的关系以及它们与环境之间的关系；
- 识别BRA设计和改进的指导原则。

BRA的核心标准化作用包括：

- 有助于制定一系列协调配套的**区块链**标准；
- 为定义**区块链**标准提供一个技术中立的参考点；
- 在识别**区块链**利益和风险时提倡开放性和透明性。

BRA重点关注**区块链**服务提供什么，而不是如何设计基于**区块链**的解决方案和实现方式。尽管BRA可能会限制某个实际系统的系统架构，但是BRA并不代表任何具体**区块链**系统的系统架构。BRA并不依赖于任何具体提供商的产品、服务或参考实现，也不定义有碍创新的常规方案。

BRA还用于：

- 帮助理解**区块链**的运营复杂性；
- 展示和理解各类**区块链**以及服务的供应和使用；
- 为社区理解、讨论、分类和比较**区块链**提供技术参考；

- 为使用通用的参考架构描述、讨论和编制系统特定的架构提供工具；
- 促进在相关领域进行潜在标准分析，同时支持后续的参考实现分析。

4 参考架构概览

本章给出了本标准所使用的体系化方法。

4.1 区块链参考架构的架构视图

区块链系统能采用视图方法进行描述。

采用四个不同的视图进行描述（见图2）：

- 用户视图；
- 功能视图；
- 实现视图；
- 部署视图。

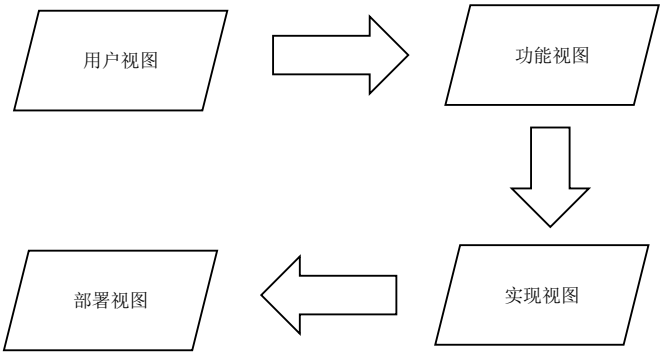


图2 不同架构视图之间的转换

表1给出对每个视图的描述。

表1 区块链参考架构视图

BRA视图	视图描述	范围
用户视图	系统环境、相关方、**角色**、**子角色**和**区块链**活动	范围内
功能视图	支撑**区块链**活动的所需功能	范围内
实现视图	实现服务、基础设施组件内的**区块链**服务所需的功能	范围外
部署视图	基于已有或新增的基础设施，对**区块链**服务功能的技术实现	范围外
注：虽然本标准包含了对用户视图和功能视图的详细描述，但并不包含对实现视图和部署视图的描述，因为实现视图和部署视图与技术，以及供应者特定的**区块链**实现和部署方式相关。		

图3给出了用户视图向功能视图的转换。详细信息见7.2节。

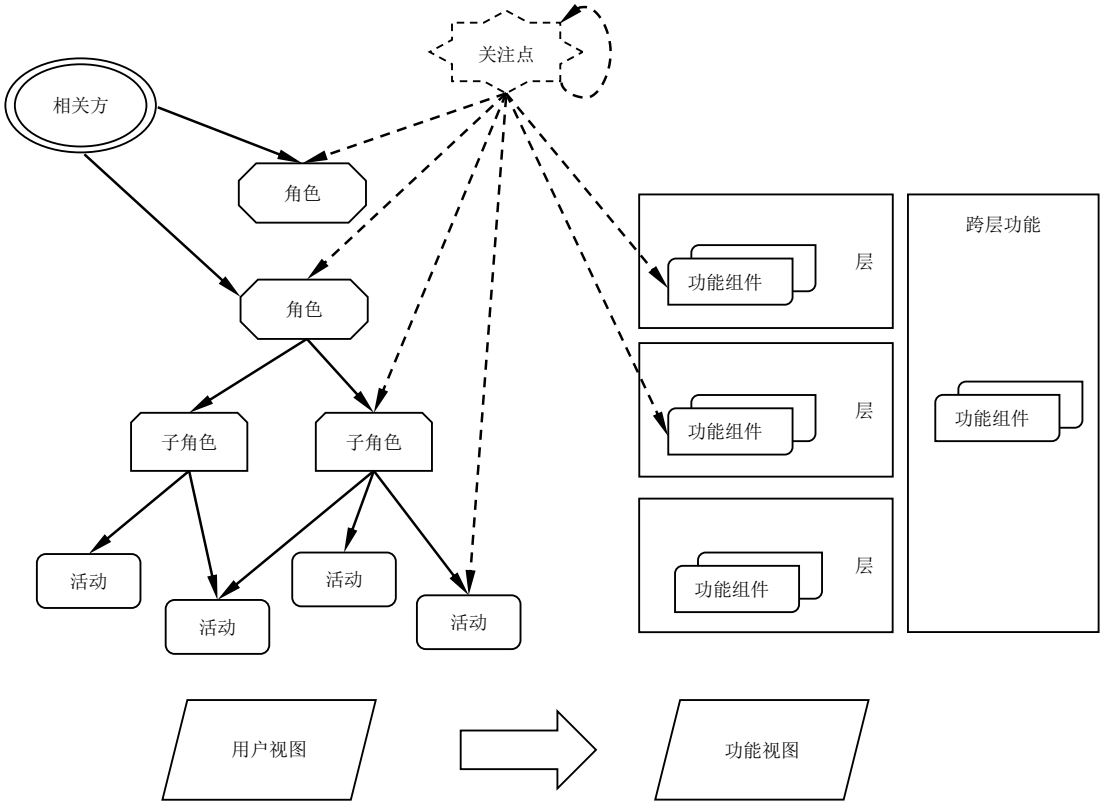


图3　用户视图向功能视图的转换

4.2　区块链用户视图

用户视图涉及以下**区块链**概念：

- **区块链活动**；
- **角色**和**子角色**；
- 相关方；
- 部署模型；
- 共同关注点。

图 4 展示了用户视图所定义的实体。

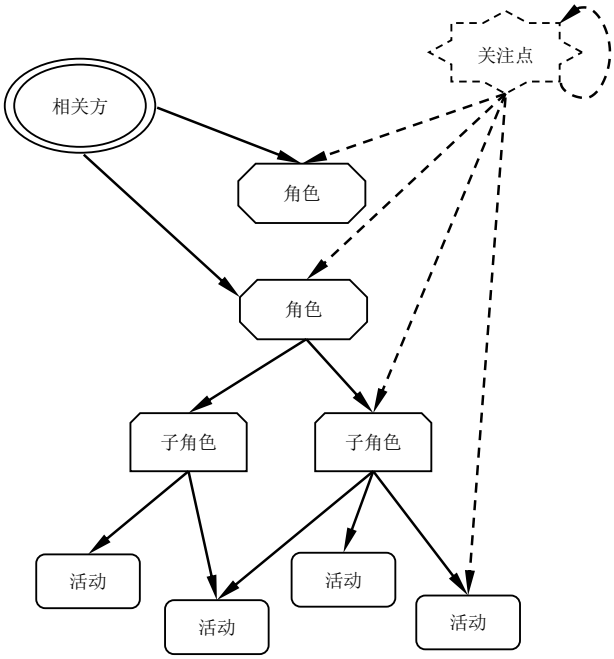


图4　用户视图实体

4.2.1　区块链活动

区块链活动定义为一组特定任务的集合。

区块链活动需要有一个目标，并能交付一个或多个结果。

区块链系统的**活动**通过**功能组件**来实现（见图 3）。

第 5 章给出**区块链活动**并进行详细描述。

4.2.2　角色和子角色

角色是一组具有共同目标的**区块链活动**的集合。

区块链参考架构定义了三个主要**角色**：

- **区块链**服务客户：使用**区块链**服务的业务相关方；
- **区块链**服务提供方：提供**区块链**服务的相关方；
- **区块链**服务关联方：为**区块链**服务提供方、**区块链**服务客户的**活动**提供支撑或辅助功能的相关方。

子角色是某个指定**角色**的**区块链活动**的子集。

某个**角色**的**区块链活动**能被该**角色**下的不同的**子角色**所共享。

第 5 章给出**区块链**的**角色**和**子角色**描述。

4.2.3　相关方

相关方是一个或一组自然人或者法人，不论该法人是否注册。**区块链**系统中的相关方是**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**，也可承担某个**角色活动**的指定子集。

4.2.4 区块链部署模型

区块链部署模型是根据对分布式账本的控制和共享方式对**区块链**进行的分类。

区块链部署模型包括：

- 公有链；
- 联盟链；
- 专有链。

附录 A 给出对**区块链**部署模型的描述。

4.2.4 共同关注点

共同关注点指的是需要在不同**角色**之间协调，且在**区块链**系统中一致实现的行为或能力。

共同关注点能被多个**角色**、**区块链活动**和**功能组件**所共享，且对他们产生影响。

共同关注点适用于多个不同的**角色**或**功能组件**。

5.5 节给出对共同关注点的描述。

4.3 区块链功能视图

功能视图是构建**区块链**系统所需功能的技术中立的视图。功能视图描述了支持**区块链活动**所需功能的分布。

功能架构还定义了功能之间的依赖关系。

功能视图涵盖了以下**区块链**概念：

- **功能组件**；
- 功能层；
- 跨层功能。

图 5 展示了功能、层和**功能组件**的概念。

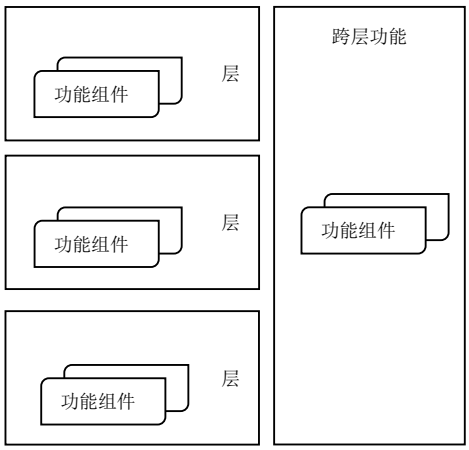


图5 功能层

6.1 节描述**区块链**功能架构。

4.3.1 功能组件

一个**功能组件**是参与某一**活动**所需的，能实现的功能构件。

区块链系统的能力完全由一组已实现的**功能组件**所定义。

6.2 节进一步描述**功能组件**。

4.3.2 功能层

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。

功能架构可部分层次化（即包含多个层和一组跨层功能）。

区块链参考架构定义了 4 个不同的层：

- 用户层；
- 服务层；
- 核心层；
- 基础层。

需要注意的是，对于某个具体的**区块链**系统，并不需要提供上述的全部**功能组件**层次。

4.3.3 跨层功能

跨层功能提供跨越多个功能层次能力的**功能组件**。跨层功能可进行分组。

已定义的跨层功能子集包括：

- 开发；
- 运营；
- 安全；
- 监管和审计。

6.2.5 描述跨层**功能组件**。

4.4 用户视图和功能视图之间关系

图 6 展示了用户视图如何提供**区块链活动**的集合，以及这些**区块链活动**在功能视图中如何表示（并通过实现视图中的技术来实现）。

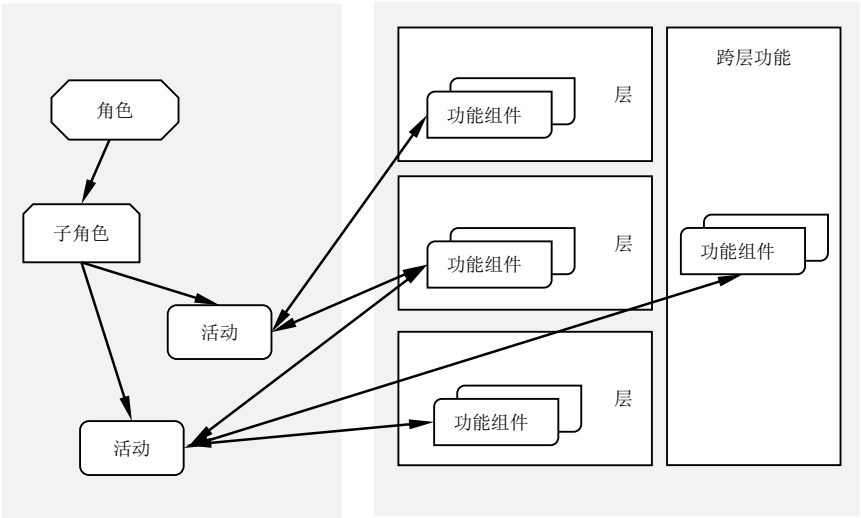


图6 从用户视图到功能视图

第 7 章进一步描述用户视图和功能视图之间的关系。

4.5 用户视图与共同关注点以及功能视图与共同关注点之间关系

如名称所示，共同关注点既适用于**区块链**的用户视图，又适用于**区块链**的功能视图。

共同关注点适用于用户视图中的**角色**和**子角色**，并且直接或间接地影响这些**角色**所执行的**活动**。

共同关注点也适用于功能视图中的**功能组件**。这些组件在执行用户视图所描述的**活动**时使用。

5.5 描述**区块链**的共同关注点。共同关注点包括：

- **模块化**（见 5.5.2）；
- 性能（见 5.5.3）；
- **互操作**（见 5.5.4）；
- 数据一致性（见 5.5.5）；
- 安全和隐私（见 5.5.6）；
- 经济合理（见 5.5.7）；
- 安全可信（见 5.5.8）。

4.6 区块链实现视图

虽然本标准详细描述了用户视图和功能视图，但是实现视图不在本标准的范围之内。

4.7 区块链部署视图

虽然本标准详细描述了用户视图和功能视图，但是部署视图不在本标准的范围之内。

5 用户视图

5.1 角色、子角色和活动概述

本章描述一些常用的与**区块链**相关的**角色**、**子角色**与他们的**活动**。

值得注意的是：在任意给定的时间点，一个相关方可承担多个**角色**。当承担一个**角色**时，相关方可限制其只承担该**角色**的一个或承担多个**子角色**。**子角色**是特定角色的所有**活动**的子集。

图 7 展示了**区块链**的**角色**及其所包含的**子角色**。其中，**区块链**的**角色**包括：

a） **区块链**服务客户（见 5.2）；

b） **区块链**服务提供方（见 5.3）；

c） **区块链**服务关联方（见 5.4）。

后续章节中详细描述图中的每一个**子角色**。

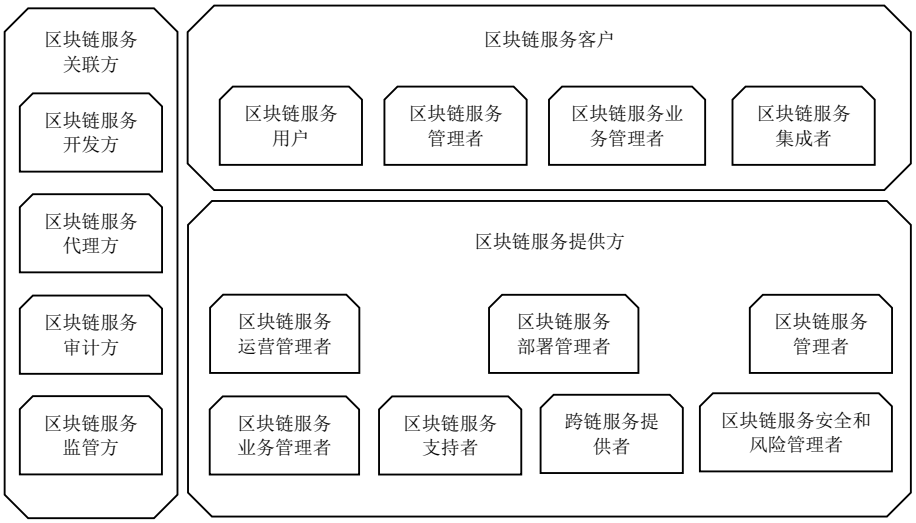


图7　区块链角色和子角色

5.2　区块链服务客户

5.2.1　角色

为使用**区块链**服务，**区块链**服务客户与**区块链**服务提供方建立业务关系。**区块链**服务客户也可由于行业背景、业务需求等原因与**区块链**服务关联方建立业务关系。

区块链服务客户的**活动**包含在5.2.1.1-5.2.1.4所描述的**子角色**中。

5.2.1.1　BSC：区块链服务用户

区块链服务用户是**区块链**服务客户的一个**子角色**。**区块链**服务用户可以是自然人，或代表企业的自然人。**区块链**服务用户与某个**区块链**服务客户相关。该**区块链**服务客户使用**区块链**服务。

区块链服务用户的**区块链活动**主要有：使用**区块链**服务（见5.2.2.1）。

5.2.1.2　BSC：区块链服务管理者

区块链服务管理者是**区块链**服务客户的一个**子角色**。**区块链**服务管理者的主要目的是保证用户使用**区块链**服务时运行稳定，同时保证**区块链**服务与**区块链**服务客户已有的业务系统和应用之间运行良好。**区块链**服务管理者监控所有与使用**区块链**服务相关的操作流程，并承担**区块链**服务客户与**区块链**服务提供方之间技术交互的切入点。

区块链服务管理者的**区块链**服务**活动**包括：

a）　测试服务（见 5.2.2.2）；
b）　监控服务（见 5.2.2.3）；
c）　安全策略管理（见 5.2.2.4）；
d）　问题处理（见 5.2.2.5）；
e）　节点管理（见 5.2.2.6）。

5.2.1.3 BSC：区块链服务业务管理者

区块链服务业务管理者是**区块链**服务客户的一个**子角色**，其目的是通过经济有效的方式获取和使用**区块链**服务，满足**区块链**服务客户的业务目标。业务管理者的主要职责是关注使用**区块链**服务时的财务和法律方面，包括审批、所有权和责任。

区块链服务业务管理者的**区块链活动**包括：

a） 业务管理（见 5.2.2.7）；

b） 隐私保护（见 5.2.2.8）；

c） 获取审计报告（见 5.2.2.9）。

5.2.1.4 BSC：区块链服务集成者

区块链服务集成者是**区块链**服务客户的一个**子角色**，负责**区块链**服务与**区块链**服务客户现有业务系统的集成、**区块链**服务之间的集成包括跨链**区块链**服务的集成，包括应用功能集成和数据交换。

区块链服务集成者的**区块链活动**主要有：跨链链接和**区块链**数据交换服务（见5.2.2.10）。

5.2.2 区块链活动

与**区块链**服务客户的**子角色**相关的**区块链活动**如图8所示。

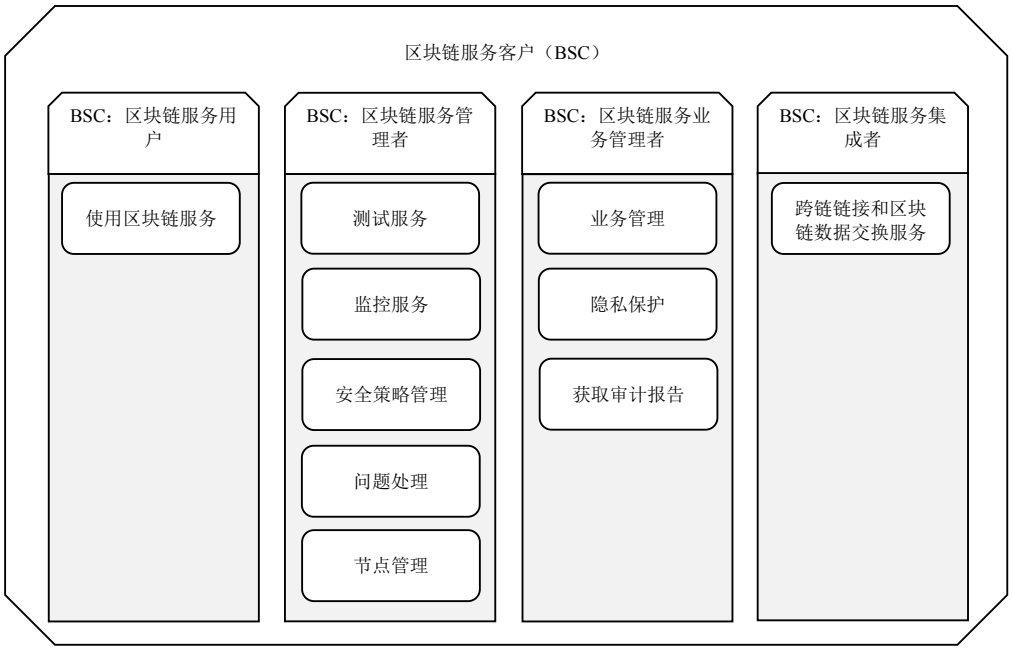


图8 与区块链服务客户的子角色相关的区块链活动

5.2.2.1 使用区块链服务

使用**区块链**服务**活动**是指**区块链**服务客户在使用**区块链**时的相关**区块链**技术服务。使用**区块链**服务**活动**的方式包括但不限于客户端、用户图形接口、命令行界面、脚本和API。该活动包括：

a） 通过客户端或用户图形接口使用**区块链**服务以执行**区块链**业务；

b） 通过命令行界面配置工具使用**区块链**服务；

c） 通过脚本自动执行使用**区块链**服务；

d） 通过API使用**区块链**服务。

5.2.2.2 测试服务

区块链测试服务**活动**指的是使用**区块链**服务提供方的测试环境服务，以确保**区块链**生产环境服务能够满足**区块链**服务客户的需求，使其在服务测试的基础上使用**区块链**服务。

测试服务**活动**应包括：

a） 提供不与生产环境**区块链**交叉的测试**区块链**，该测试**区块链**应具备与生产环境**区块链**相同功能及服务；

b） 生成若干模拟用户以开展相关测试；

c） 在联盟链和专有链中，应允许**区块链**服务能够认证用户并赋予对测试**区块链**服务客户的访问权限；

d） 满足**区块链**服务客户对**区块链**服务进行业务、技术需求的测试。

5.2.2.3 监控服务

监控服务**活动**主要为保障及监测**区块链**服务的运行状况和**区块链**服务客户情况，贯穿**区块链**的各个环节，通过对节点及数据的跟踪发现系统中存在的问题，实现对系统性能质量的控制。该**活动**包括：

a） 跟踪每个**区块链**节点的共识、数据同步以保证适宜的**区块链**服务使用量；

b） 监控**区块链**服务与**区块链**服务客户现有系统的集成，以确保业务目标的满足；

c） 定义服务的测量点和性能指标（例如：服务可靠性、服务可用性、平台的响应性)；

d） 监控、分析和归档指标数据。

5.2.2.4 安全策略管理

安全策略管理**活动**主要为确保存放在**区块链**计算环境中的**区块链**服务客户数据的安全性，确保整个区块链网络、计算和存储环境面向用户的可用性。该活动包括：

a） 制定口令校验、**数字签名**校验、生物特征识别校验等确保用户和节点身份真实性的身份鉴别方法；

b） 制定确保**区块链**数据备份和恢复，以及可能的数据复制和故障转移的计划；

c） 选择适用于静态和动态**区块链**服务客户数据的**加密**和完整性技术；

d） 制定可选的系统密钥保障方案。

5.2.2.5 问题处理

问题处理**活动**包括对用户使用**区块链**服务过程中相关问题的处理，具体包括：

a） 评估问题的影响程度和影响范围；

b） 通过故障排查，找到问题的原因；

c） 寻找问题解决办法，启动相应的问题排除机制，并持续跟踪至问题解决；

d） 针对在约定时间内无法通过业务层面的操作完成修复或对业务具有严重影响的问题通过系统升级予以解决；

e） 问题的标识、记录、存档和备查。

5.2.2.6 节点管理

节点管理**活动**管理**区块链**服务提供方创建的**区块链**服务对象。该**活动**包括：

a） 对节点功能的配置和控制，包括账本、共识、数据**加密**、身份识别等；

b） 管理同一节点上不同**区块链**服务客户共享数据的访问控制；

c） 管理验证交易，维护账本的数据一致写入状态；

d） 确保**区块链**网络拓扑结构支持节点的动态增减；

e） 确保区块链基础设施满足不同节点的要求。

5.2.2.7 业务管理

业务管理**活动**包括对使用**区块链**服务的业务方面进行管理，包括会计和财务管理，具体包括：

a） 调整业务计划以适应**区块链**服务的使用；
b） 跟踪服务的使用，处理会计和财务管理；
c） 处理因使用**区块链**服务而收到的来自**区块链**服务提供方的帐单/发票；
d） 确保帐单和**区块链**服务客户的实际**区块链**服务使用情况相匹配；
e） 向**区块链**服务提供方支付；
f） 培养相关人员对**区块链**业务进行操作；
g） 记录与使用**区块链**服务相关的帐务。

5.2.2.8 隐私保护

由于**区块链**技术为所有的参与节点提供了公共账本，这给业务的使用者和提供者带来了额外的隐私挑战。隐私保护**活动**具体包括：

a） 识别**区块链**服务的隐私构成；
b） 制定**区块链**服务隐私保护策略；
c） 执行具体的**区块链**隐私保护**活动**，对构成隐私的事务相关的相关方身份和事务细节的保护，具体的保护对象包括并不限于数据存储、数据传输和数据应用；
d） 定期审核**区块链**隐私保护策略和隐私保护**活动**的具体效果，必要时对隐私保护策略进行修订，并按照新的策略执行隐私保护**活动**。

5.2.2.9 获取审计报告

获取审计报告**活动**指的是**区块链**服务业务管理者通常遵循特定的审计标准或方案，获取**区块链**服务的审计报告。**区块链**服务业务管理者可向**区块链**审计方获取报告。审计报告既在服务购买完成前提供，又在服务使用中定期提供。具体**活动**应包括：

a） 根据监管和业务发展要求，制定审计标准和方案，并在内部实施审计和形成审计报告，必要时应对**区块链**服务提供方实施审计；
b） 根据监管和业务发展要求，接受**区块链**服务关联方中审计方的审计并获取审计报告（具体**活动**见 5.4.1.3）。

5.2.2.10 跨链链接和区块链数据交换服务

跨链链接和**区块链**数据交换服务**活动**指集成现有的**区块链**应用和数据到其他系统，既包括集成现有的**区块链**应用和数据到目标**区块链**系统，又包括集成**区块链**应用和数据到目标非**区块链**系统，如**区块链**服务提供方的监控和管理系统。

跨链数据的交换可通过数据适配器或在链上发行对等数据内容等方式来实现。

跨链链接和**区块链**数据交换服务**活动**包括：

a） 评估**区块链**应用对现有待接入目标系统的流程和服务的影响；
b） 建立现有待接入目标系统与**区块链**应用之间的业务数据映射；
c） 在现有待接入目标系统中调用**区块链**服务，包括提供**区块链**服务输入数据，处理**区块链**服务输出数据；
d） 为**区块链**服务用户提供访问权限；
e） 定义和实现安全相关的需求，包括数据流的保密性和完整性；

f） 集中管理用户帐号、安全**角色**，身份和许可权的客户设施和管理**区块链**服务的对等设施；
g） 创建和监控使用**区块链**服务管理接口的特定用户帐号和身份；
h） 集成**区块链**服务与**区块链**服务客户的监控和管理基础设施之间的登录和安全事件管理；
i） 如果连接和数据交换是双向的，还需在现有**区块链**应用中调用待接入目标系统服务，包括提供待接入目标系统服务输入数据，处理待接入目标系统服务输出数据，为待接入目标系统服务用户提供访问权限，集中管理用户帐号、安全**角色**，身份和许可权的客户设施和管理**区块链**服务的对等设施，创建和监控使用待接入目标系统服务管理接口的特定用户帐号和身份，集成待接入目标系统服务与待接入目标系统服务客户的监控和管理基础设施之间的登录和安全事件管理。

5.3 区块链服务提供方

5.3.1 角色

5.3.1.1 BSP：区块链服务运营管理者

BSP：**区块链**服务运营管理者是**区块链**服务提供方的**子角色**，负责执行**区块链**服务提供方的所有运营过程和流程，确保所有的服务和相关的基础设施满足运营目标。

BSP：**区块链**服务运营管理者的**活动**包括：

a） 准备系统（见 5.3.2.1）；
b） 监控和管理服务（见 5.3.2.2）；
c） 管理资产和库存（见 5.3.2.3）；
d） 提供审计数据（见 5.3.2.4）。

5.3.1.2 BSP：区块链服务部署管理者

BSP：**区块链**服务部署管理者是**区块链**服务提供方的**子角色**，负责规划和实施**区块链**服务部署**活动**。该**活动**包括定义服务运维环境、定义服务运行的度量指标和采集方式、定义服务运行过程的依赖资源和可用的运维流程。

BSP：**区块链**服务部署管理者的**活动**包括：

a） 定义环境和流程（见 5.3.2.5）；
b） 定义度量指标和指标采集方法（见 5.3.2.6）；
c） 定义部署步骤（见 5.3.2.7）。

5.3.1.3 BSP：区块链服务管理者

BSP：**区块链**服务管理者是**区块链**服务提供方的**子角色**，负责确保**区块链**服务客户使用**区块链**服务提供方的**区块链**服务时，服务功能正确并且和SLA描述的目标一致。**区块链**服务管理者还负责确保**区块链**服务提供方的业务支撑系统和运营支撑系统运营稳定，以及向**区块链**服务客户和**区块链**服务关联方提供的各项**活动**运营稳定。

BSP：**区块链**服务管理者的**活动**包括：

a） 提供服务（见 5.3.2.8）；
b） 部署和配置服务（见 5.3.2.9）；
c） 服务水平管理（见 5.3.2.10）。

5.3.1.4 BSP：区块链服务业务管理者

BSP：**区块链**服务业务管理者是**区块链**服务提供方的**子角色**，整体负责向**区块链**服务客户提供**区块链**服务的业务方面管理，如创建和跟踪业务计划，定义服务供应策略，管理和服务客户之间的业务关系。

BSP：**区块链**服务业务管理者的**活动**包括：

a） 管理业务规划（见 5.3.2.11）；

b） 管理客户关系（见 5.3.2.12）；

c） 管理财务处理流程（见 5.3.2.13）。

5.3.1.5 BSP：区块链服务支持者

BSP：**区块链**服务支持者是**区块链**服务提供方的**子角色**，是**区块链**服务客户和**区块链**服务提供方之间的主要接口，负责及时、高成本效益地对客户的问题和咨询做出响应，以维护**区块链**服务提供方及其提高**区块链**服务的客户满意度。

BSP：**区块链**服务支持者的**区块链**服务**活动**主要有：响应客户请求（见5.3.2.14）。

5.3.1.6 BSP：区块链跨链服务提供者

BSP：跨链服务提供方是**区块链**服务提供方的**子角色**。该**子角色**依靠一个或者多个**区块链**服务提供方向**区块链**服务客户提供部分或者全部**区块链**服务。从**区块链**服务客户的角度看，跨链服务提供者让客户能够同时使用多个**区块链**服务提供方的服务，**区块链**服务客户能够只使用跨链服务提供者的服务实现其业务目标。

BSP：跨链服务提供者的**活动**包括：

a） 管理同级的**区块链**服务（见 5.3.2.15）；

b） 互连、联合、聚合、强化和仲裁（见 5.3.2.16）。

5.3.1.7 BSP：区块链服务安全和风险管理者

BSP：**区块链**服务安全和风险管理者是**区块链**服务提供方的**子角色**，负责确保**区块链**服务提供方能恰当地管理与**区块链**服务的开发、交付、使用和支撑相关的风险，确保**区块链**服务客户的信息安全策略和**区块链**服务提供方的信息安全策略相一致，并能满足SLA中的安全需求。

BSP：**区块链**服务安全和风险管理者的**活动**包括：

a） 管理安全和风险（见 5.3.2.17）；

b） 设计和实现服务的连续性（见 5.3.2.18）；

c） 确保合规性（见 5.3.2.19）。

5.3.2 区块链活动

与**区块链**服务提供方的**子角色**相关的**区块链活动**如图9所示。

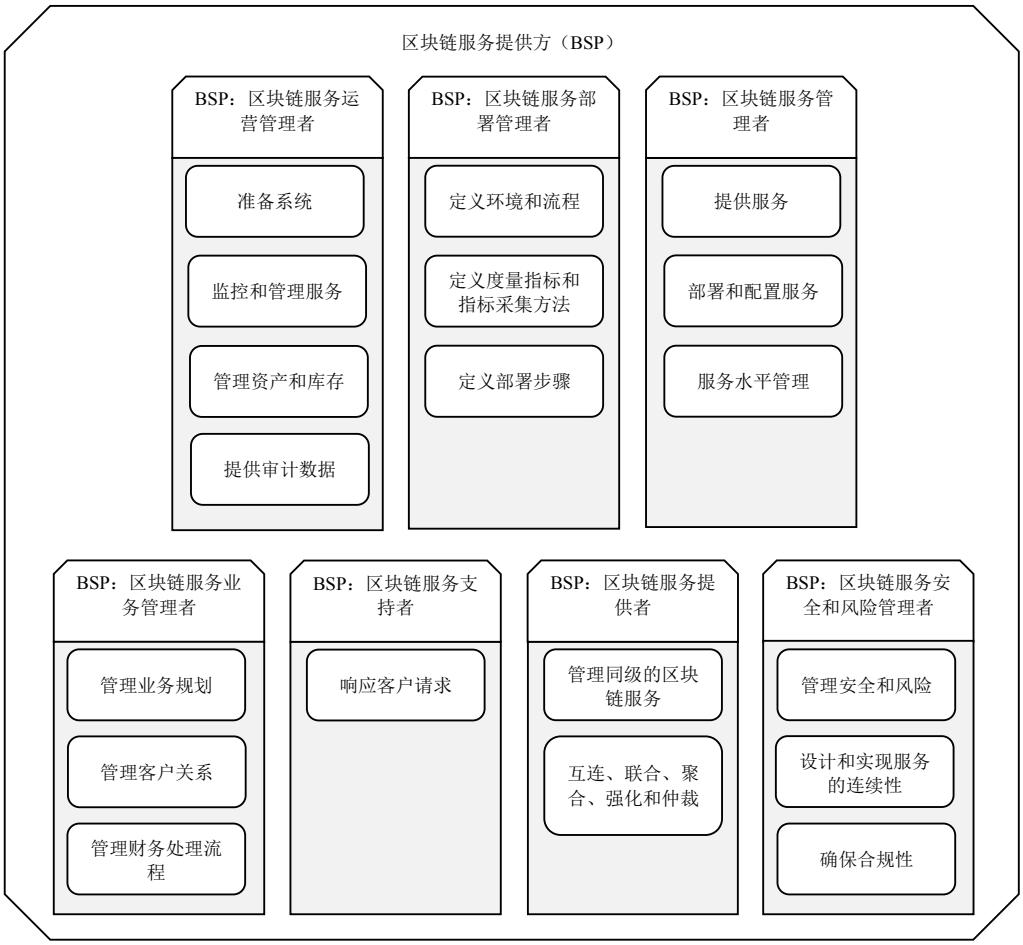


图9　与区块链服务提供方的子角色相关的区块链活动

5.3.2.1　准备系统

准备系统**活动**主要是为部署新的服务，在**区块链**服务提供方环境中所做的系统准备工作。该**活动**包括：

a）　评估新服务的部署或已有服务的增长所带来的影响；

b）　修改节点的配置，或新增节点，以满足新的部署需求。

5.3.2.2　监控和管理服务

监控和管理服务**活动**关注于监控和管理服务及相关的基础设施，包含用户权限和系统权限。该**活动**包括：

a）　监控**区块链**服务提供方的服务和基础设施；

b）　获取对**区块链**服务提供方业务重要的事件和数据，并根据需求将数据提供给**区块链**服务业务管理者。此类数据包括**区块链**服务客户的**区块链**服务使用情况和**区块链**服务的供应成本等；

c）　分配和管理存储资源；

d）　管理用户、系统及节点权限；

e）　监控**区块链**服务提供方的**区块链**服务环境，以确保该环境正常运行和所提供的服务符合 SLA 中的条款；

f） 记录和适时地报告问题（可能涉及向一个或多个客户发送问题消息），并跟踪问题处理流程，直到问题解决。

5.3.2.3 管理资产和库存

管理资产和库存**活动**包括：

a） 跟踪计算、存储、网络和软件资产的多个方面，例如版本和补丁信息，相关的配置信息等；

b） 新资产的上线和旧资产的回收。这一过程可包括确保新上线的资产符合使用目的，且对安全性和可管理性进行适当的检查，也包括对不再需要资产的处理。这一过程可包含对保存数据的所有资产进行适当的安全处理。

5.3.2.4 提供审计数据

提供审计数据**活动**是指对与审计请求相关的数据的收集和提供，例如系统的安全控制日志，服务的监控数据等。审计数据的内容取决于所使用的审计方案或标准。该**活动**包括：

a） 根据日志等数据生成和发送合适的审计信息；

b） 基于日志记录，或可能包含敏感信息或个人识别信息（PII）的数据编写信息。

5.3.2.5 定义环境和流程

定义环境和流程**活动**关注于定义服务运行所需的技术环境和操作流程。该**活动**包括：

a） 定义服务运行所需的技术环境，包括计算、存储和网络资源，以及服务所依赖的软件和相应的配置；

b） 确保**区块链**服务符合安全性和业务合规性相关的标准；

c） 定义服务运行所遵循的流程，包括问题修复、升级和迁移流程等。

5.3.2.6 定义度量指标和指标采集方法

定义度量指标和指标采集方法**活动**关注于定义服务水平指标和管理。该**活动**包括：

a） 定义与**区块链**服务运营相关的指标，如服务响应时长、系统吞吐量、服务可用率等，并将定义的指标纳入**区块链** SLA 的条款中；

b） 设计每个**区块链**服务的指标的收集方法；

c） 定义如何报告和管理服务指标，以确保满足 SLA 的目标。

5.3.2.7 定义部署步骤

定义部署步骤**活动**关注于定义服务部署的步骤。该**活动**描述运维和支撑团队为实现服务部署并正常运行所采取的步骤。

定义部署步骤**活动**包括：定义服务运行时的状态监控，及保证服务对**区块链**服务客户可用所需采取的策略及流程。

5.3.2.8 提供服务

提供服务**活动**包括将**区块链**服务交付给**区块链**服务客户所需的所有步骤。提供服务**活动**包括：

a） 接受和处理经过授权和认证的用户的服务调用请求；

b） 管理服务的异常处理过程；

c） 管理运营系统；

d） 维护服务和底层的基础设施；

e） 自动化系统流程；

f） 管理长期的容量趋势和性能走势；
g） 安装、配置和维护**区块链**服务所需的硬件，包括计算、存储和网络通信能力；
h） 安装、配置和维护**区块链**服务所需的软件。根据需要对软件进打补丁、更新和升级。

5.3.2.9 部署和配置服务

部署和配置服务**活动**包括将已实现的服务投入运行使得服务使用者可通过网络终端访问服务，以及能够处理来自用户的服务请求。

部署和配置服务**活动**包括：依据为服务定义的部署流程对服务进行部署和配置。

5.3.2.10 服务水平管理

服务水平管理**活动**主要管理服务与 SLA 条款之间的依从性。该**活动**包括：

a） 监控每个服务的指标，并与该服务 SLA 中定义的服务水平进行对比；
b） 当服务指标不符合 SLA 中定义的水平时，采取相应的措施使其与 SLA 保持一致，例如，执行由**区块链**服务部署管理者定义的处理流程；
c） 当服务无法达到与 SLA 一致的水平时，报告问题。

5.3.2.11 管理业务规划

管理业务规划**活动**包括：

a） 定义服务交付，描述服务交付的技术方面（如功能接口、SLA 等）和业务方面；

注：当建立服务交付时，**区块链**服务提供方可能需要考虑与对等的服务提供者之间的交互。

b） 创建业务规划，包括以下方面：为客户交付一个或多个**区块链**服务、处理服务的财务和技术方面内容、目标客户群、合约和 SLA、市场渠道和销售目标等；
c） 根据业务规划，跟踪销售和服务使用情况，以确保**区块链**服务提供方财务目标的实现；
d） 为提供**区块链**服务准备和调整业务规划。

5.3.2.12 管理客户关系

管理客户关系**活动**包括对**区块链**服务提供方和**区块链**服务客户之间业务关系的管理，具体包括：

a） 创建和维护产品目录的内容；
b） 获取客户；
c） 为客户提供各项业务事宜的联系方式；
d） 讨论并解决客户的顾虑或问题；
e） 处理客户的需求变更请求（例如，客户权利的变更）。

5.3.2.13 管理财务处理流程

管理财务处理流程**活动**包括：

a） 处理账单更新或客户对账单的疑问；
b） 处理服务合同中的费用相关问题；
c） **区块链**服务提供方生成与**区块链**服务使用相关的账单信息和/或发票，并将其发送给**区块链**服务客户；
d） 收取**区块链**服务客户支付的费用，与**区块链**服务客户进行费用核算。

5.3.2.14 响应客户请求

响应客户请求**活动**包括：处理**区块链**服务客户发来的服务请求和报告。**区块链**服务提供方可向客户

提供多种与服务支持人员交流的方式，如论坛、电子邮件、客户支持桌面系统、Web 门户、即时通信等。

注：一些请求或报告可能只要求提供信息，或详细说明，其他的请求和报告可能要求对问题的分析，或者是需求变更申请。

5.3.2.15 管理同级的区块链服务

管理同级**区块链**服务**活动**关注对一个同级**区块链**服务提供方的**区块链**服务的管理。该**活动**包括：

a） 选取和使用一个同级**区块链**服务提供方的一个或者多个**区块链**服务；

b） 监控同级**区块链**服务提供方的**区块链**服务；

c） 跟踪同级**区块链**服务提供方的**区块链**服务的使用情况；

d） 在**区块链**服务客户和所有同级的**区块链**服务提供方之间协调身份。

5.3.2.16 互连、联合、聚合、强化和仲裁

互连、联合、强化、聚合和仲裁**活动**是指按如下特定的方式使用同级**区块链**服务提供方的**区块链**服务：

a） 互连是指使用一个同级**区块链**服务提供方的**区块链**服务；

b） 联合是指使用一组同级**区块链**服务提供方的**区块链**服务，组合这组**区块链**服务提供方的服务能力，来提供**区块链**服务客户需要的一组**区块链**服务；

c） 聚合是指**区块链**服务提供方通过组合同级**区块链**服务提供方提供的一组**区块链**服务以提供一个**区块链**服务；

d） 强化是指**区块链**服务提供方通过调整或增强同级**区块链**服务提供方的**区块链**服务来提供**区块链**服务；

e） 仲裁是指**区块链**服务提供方从同级服务提供方提供的一组**区块链**服务中进行选择从而提供**区块链**服务。

5.3.2.17 管理安全和风险

管理安全和风险**活动**主要关注与**区块链**服务的开发、交付、使用和支持相关的安全和风险管理。该**活动**包含：

a） 定义信息安全策略，需要考虑服务需求、法令法规需求、合同和 SLA 要求；

b） 定义与**区块链**服务相关的信息安全风险，以及为满足**区块链**服务提供方的业务目标而对这些风险所采取的解决办法。从节省成本出发，提供者也可从业务的角度考虑自己不处理一些风险，而通过服务协议的方式，交给**区块链**服务客户处理，以满足部分市场的成本需求；

c） 为解决与所选的服务和设计点相关的风险，选取设计点和相关的信息安全控制。信息安全控制通常包括但不限于以下内容：

1） 身份和访问管理；

2） 发现、分类、保护数据和信息资产；

3） 信息系统的获取、开发和维护；

4） 对威胁和漏洞安全的基础设施；

5） 问题和信息安全事件管理；

6） 安全治理和合规性；

7） 物理安全和人员安全；

8） 网络安全和通信安全；

9） 隔离性。

d） 确保为部署的服务和底层的基础设施落实可识别的信息安全控制；

e） 设计、实现和评价系统和应用的安全性；
f） 管理、设计、实现和评价对等**区块链**服务提供方的**区块链**服务安全性；
g） 评价已实现的信息安全控制的有效性，并基于经验做相应的调整。

5.3.2.18 设计和实现服务连续性

设计和实现服务连续性**活动**主要有：考虑到**区块链**服务和支撑基础设施的潜在故障和应急模式，通过诸如故障转移和冗余等技术，落实恢复流程，使得**区块链**服务在 SLA 条款内可用。

5.3.2.19 确保合规性

确保合规性**活动**主要实现对法规合规性和标准合规性的支持。该**活动**包括：
a） 确保**区块链**服务和支撑基础设施的实现满足所有需要支持的标准的需求，例如，目标客户群要求的标准，或者提供者用来保证服务所选择的认证体系所要求的标准；
b） 确保**区块链**服务和支撑基础设施的实现（包括数据处理）满足对服务或服务所存储或处理数据的所有法规需求。

5.4 区块链服务关联方

5.4.1 角色

区块链服务关联方是为**区块链**服务提供方和/或**区块链**服务客户的**活动**提供支撑或辅助功能的相关方。

区块链服务关联方的**活动**随着合作者的类型及其与**区块链**服务提供方和**区块链**服务客户之间关系的不同而变化。

5.4.1.1 BSR：区块链服务开发方

区块链服务开发方是**区块链**服务关联方的**子角色**，负责基于**区块链**系统提供各类业务服务功能的设计、开发、测试和维护。可能涉及根据现有服务的实现或现有的系统来组合服务实现。

区块链服务开发方的**活动**包括：
a） 设计、创建和维护**区块链**系统中的服务组件或**智能合约**（见 5.4.2.1）；
b） 设计、创建、集成和维护基于**区块链**系统的业务服务系统（见 5.4.2.2）；
c） **区块链**系统中的服务组件组合服务（见 5.4.2.3）；
d） **区块链**系统中的服务组件测试服务（见 5.4.2.4）。

5.4.1.2 BSR：区块链服务代理方

区块链服务代理方是**区块链**服务关联方的**子角色**，负责在**区块链**服务客户和其他**区块链**服务提供方之间进行协商。**区块链**服务代理方不提供与**区块链**服务提供方环境中的**区块链**技术支持能力。

区块链服务代理方的**活动**包括：
a） 获取和评估客户（见 5.4.2.5）；
b） 评估市场（见 5.4.2.6）；
c） 设立法律协议（见 5.4.2.7）。

5.4.1.3 BSR：区块链服务审计方

区块链服务审计方是**区块链**服务关联方的**子角色**，负责审计**区块链**服务的供应和使用。**区块链**服务审计通常覆盖运营、性能和安全，主要是检查相关的审计准则是否得到满足。

区块链服务审计方的**活动**包括：
a） 选择**区块链**服务的审计形式（见 5.4.2.8）；

b） 执行**区块链**服务审计（见 5.4.2.9）；

c） 报告审计结果（见 5.4.2.10）。

注：审计相关**活动**应在保护隐私的前提下进行。

5.4.1.4 BSR：区块链服务监管方

区块链监管方是重要的**区块链**合作者之一，负责监督管理**区块链**服务提供方及其他**区块链**服务相关方，维护**区块链**服务的合法、稳健运行，维护客户对**区块链**服务的信心。

区块链监管方的主要**活动**包括：

a） 制定规则（见 5.4.2.11）；

b） 审批和报备（见 5.4.2.12）；

c） 现场和非现场监管（见 5.4.2.13）；

d） 应急管理（见 5.4.2.14）；

e） 统计报表（见 5.4.2.15）。

注：监管相关**活动**应在保护隐私的前提下进行。

5.4.2 区块链活动

与**区块链**服务关联方的**子角色**相关的**区块链活动**如图10所示。

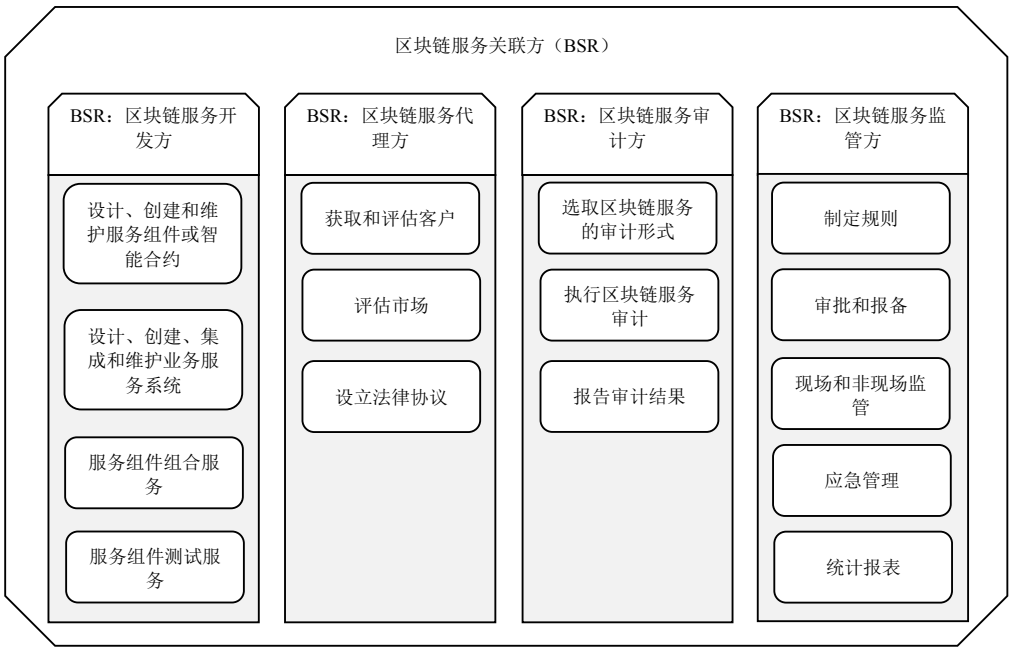


图10 与区块链服务关联方的子角色相关的区块链活动

5.4.2.1 设计、创建和维护区块链系统中的服务组件或智能合约

设计、创建和维护**区块链**系统中的服务组件或**智能合约活动**涉及如下内容：

a） 设计和创建用于服务实现的符合**区块链**系统要求的服务代码或**智能合约**代码；

b） 描述服务的技术方面（例如功能接口，SLA）；

c） 为服务使用方设计使用服务功能的接口；

d） 处理与**区块链**系统中的服务功能实现的运维功能和相关的问题报告；

e） 提供对**区块链**系统中的服务功能实现的修正及异常处理能力；
f） 提供对**区块链**系统中的服务功能实现的扩展能力；
g） 提供对**区块链**系统中的服务功能的说明与审核支持功能，宜包括源代码审计。

5.4.2.2 设计、创建和维护基于区块链系统的业务服务系统

设计、创建和维护基于**区块链**系统的业务服务系统**活动**涉及如下内容：
a） 设计和创建用于服务实现的基于**区块链**系统的业务服务系统，业务服务系统通过接口等交互机制与**区块链**系统交互，业务系统不是**区块链**系统的组成部分；
b） 处理业务系统与**区块链**系统共同运维的功能与相关的问题报告；
c） 提供对业务系统与**区块链**系统中集成功能实现的修正能力；
d） 提供对业务系统与**区块链**系统中集成功能实现的扩展能力；
e） 提供对基于**区块链**系统的业务服务系统的说明与审核支持功能，宜包括与**区块链**系统集成部分源代码审计。

5.4.2.3 区块链系统中的服务组件组合服务

区块链系统中的服务组件组合服务**活动**主要关注通过已有**区块链**系统中的服务组合新的服务。该**活动**包括：
a） 通过组合已有的一个或多个**区块链**系统中服务功能来创建新的服务功能；
b） 描述服务的技术方面（例如功能接口，SLA）；
c） 为服务使用者设计集成的接口使其能访问多个**区块链**系统服务功能；
d） 提供对组合服务功能的说明以及审核支持功能，宜包括源代码审计。

注 1：组合可包括对已有服务的强化、聚合或扩展。

注 2：组合服务不应对原有单项服务功能产生影响。

5.4.2.4 区块链系统中的服务组件测试服务

区块链系统中的服务组件测试服务**活动**主要关注于**区块链**系统中服务功能的测试。该**活动**包括：
a） 对**区块链**系统中实现的组件功能进行测试，以确保这些组件完整并正确地实现了服务功能；
b） 对**区块链**系统中实现的组件功能进行测试，以检测这些组件的系统安全性与健壮性；
c） 确保服务功能接口的**互操作**性；
d） 测试宜覆盖**区块链**系统中的服务部署节点。

5.4.2.5 获取和评估客户

获取和评估客户**活动**包括为销售**区块链**服务所需的各种任务，此时**区块链**服务客户签订协议同意使用一个或多个服务。该**活动**包括：
a） 为潜在客户提供关于可用的服务、相关的 SLA 以及合同条款的相关信息；
b） 与客户协商服务条款和价格；
c） 评估客户对**区块链**服务的需求。

注：区块链服务客户的需求评估**活动**包括为确定和解决**区块链**服务客户的需求所采取的措施。其中，**区块链**服务客户的需求在对客户现有能力和预期能力进行差距分析的基础上标识。

5.4.2.6 评估市场

评估市场**活动**主要关注于评估当前的**区块链**服务市场和生态系统，从而为客户寻找符合其需求的**区块链**服务。该**活动**包括：

a） 对**区块链**服务提供方所供应的产品进行调研，获取技术信息和商业信息；
b） 订阅和接受**区块链**服务提供方产品目录内容变更的通知；
c） 对产品供应和**区块链**服务客户需求进行匹配，匹配内容包括技术、商业和法规等方面。

5.4.2.7 创建合法协议

创建合法协议**活动**主要关注于**区块链**服务客户与所选定的**区块链**服务提供方之间的服务协议。该**活动**包括**区块链**服务客户和所选的**区块链**服务提供方之间为满足客户需求，对服务协议进行的协商。

5.4.2.8 选择区块链服务的审计形式

区块链服务审计的形式有以下两种选择：
a） **区块链**服务审计方作为审计节点接入**区块链**网络，实时获得**区块链**网络中的数据与证据；
b） **区块链**服务审计方作为**区块链**网络之外的第三方机构，按需或定时获得**区块链**网络中的数据与证据。

5.4.2.9 执行区块链服务审计

执行**区块链**服务审计**活动**包括：
a） 请求或获取审计证据；
b） 可在待审计的**区块链**网络上进行任何需要的测试；
c） 选择成为待审计的**区块链**网络的一个节点，实时获取审计证据；
d） 选择作为**区块链**网络之外的第三方机构，通过待审计的**区块链**网络提供的一组接口，以程序调用的方式获取审计证据；
e） 在必要时可修改审计证据，以保护敏感信息或受法规控制的信息；
f） 对比所用的审计方案或审计标准中描述的审计准则和获得的审计证据。

5.4.2.10 报告审计结果

报告审计结果**活动**以文档报告形式提供审计结果。文档报告的形成取决于正在使用的审计方案，审计结果可根据业务场景或法律法规，提交给**区块链**服务业务管理者。

5.4.2.11 制定规则

制定规则**活动**主要关注于依照法律、行政法规，制定并发布对**区块链**服务提供方及业务**活动**监督管理的规章规则，包括用户管理、业务品种、链上资产管理、**智能合约**、账本记录、架构管理、开发管理、运营管理、信息安全、风险管理、从业资格等内容。

5.4.2.12 审批和报备

审批和报备**活动**包括：
a） 审批**区块链**服务监管方的设立、变更、终止及其业务范围，应对**区块链**服务提供方**区块链**服务能力、风险状况、诚信状况等进行审查；
b） 对**区块链**服务提供方的高级管理人员实行任职资格管理。

5.4.2.13 现场和非现场监管

现场和非现场监管**活动**包括：
a） 应对**区块链**服务提供方业务**活动**及其风险状况，进行现场和非现场监管，分析、评价**区块链**风险状况；

b） 根据履行职责的需要，**区块链**服务监管方有权要求**区块链**服务提供方按照规定报送**区块链**服务提供情况、信息安全情况以及**区块链**服务审计方出具的审计报告；可以与**区块链**服务提供方高级管理人员进行监督管理谈话，要求**区块链**服务提供方高级管理人员就其业务**活动**和风险管理的重大事项作出说明；

c） 应要求**区块链**服务提供方按照规定，如实向**区块链**服务客户披露风险管理状况、高级管理人员变更以及其他重大事项等信息；

d） **区块链**服务提供方违反规则的，**区块链**服务监督方应责令限期改正；逾期未改正的，或者其行为严重危及**区块链**服务提供方的稳健运行、损害其他**区块链**服务提供方或客户合法权益的，**区块链**服务监管方可以区别情形，采取暂停部分业务、停止批准开办新业务、终止业务等措施；

e） 应制定检查程序，规范检查行为。

5.4.2.14 应急管理

应急管理**活动**包括：

a） 应建立**区块链**突发事件的发现、报告制度；

b） 发现可能引发系统性风险、严重影响社会稳定的突发事件的，应立即向国家有关部门报告；

c） 应会同**区块链**提供方及有关部门建立突发事件处置制度，制定**区块链**突发事件处置预案，明确处置机构和人员及其职责、处置措施和处置程序，及时、有效地处置**区块链**突发事件。

5.4.2.15 统计报表

统计报表**活动**包括：负责编制**区块链**服务统计数据、报表，并按照有关规定予以公布。

5.5 共同关注点

5.5.1 概述

共同关注点包括**区块链**系统的架构层面和运营层面，适用于 BRA 描述范围内或与 BRA 的实例系统运营相关的多个元素，并在多个**角色**、**活动**和**功能组件**中共享。

共同关注点常常影响到**角色**所执行的**活动**。为了支持某个共同关注点，需要协调不同**角色**和同一**角色**的不同**活动**。支持共同关注点还需要支持**区块链活动**、技术能力和实现的组件。针对每个共同关注点，需要定义一组**区块链活动**和组件。不同的**角色**和解决方案可能使用这些共同关注点的不同子集。

共同关注点包括：

a） **模块化**（见 5.5.2）；

b） 性能（见 5.5.3）；

c） **互操作**（见 5.5.4）；

d） 数据一致性（见 5.5.5）；

e） 安全和隐私（见 5.5.6）；

f） 经济合理（见 5.5.7）；

g） 安全可信（见 5.5.8）。

5.5.2 模块化

为了提高**区块链**应用的研发效率、可维护性和可移植性，**区块链**系统的核心功能应实现**模块化**、可配置和可扩展，以便快捷地构建上层应用。

5.5.3 性能

性能指的是某个**区块链**系统在一段约定的时间内执行相关功能的能力。从客户角度看，性能通常是

区块链系统的一个关键属性，也是当前关注的焦点。

构建**区块链**系统，提供**区块链**服务，应注重提升**区块链**系统的吞吐量，以满足主流交易网络高并发的性能要求。

5.5.4 互操作

区块链语境下的**互操作**指：

a） **区块链**服务客户与**区块链**服务之间按照规定的方法交互和交换信息并获得可预测结果的能力，以及**区块链**服务提供方与其他**区块链**服务提供方之间协同工作的能力；

b） 要求**区块链**服务按照商定的规范运营，并采用通用的**分布式账本技术**，避免使用专有的或高度专业化软件；

c） 延伸到**区块链**服务本身之外，**互操作**还包括**区块链**服务客户与**区块链**服务提供方的管理设施的交互。

d） 在业务运用中，**互操作**还会涉及到传统 IT 应用与**区块链**服务之间交互的能力，应采用统一的通信协议和 API 进行交互。

实现不同**区块链**间的**互操作**，应采用有效的通信协议、统一的 API 和区块数据格式，以及高效的连接机制。

5.5.5 数据一致性

数据一致性是实现**区块链**服务**互操作**和可移植的前提。

实现数据一致性，应采用科学合理的数据算法，降低数据同步延迟，保证数据的一致性，避免造成数据混乱和失准，并减少意外分叉带来的风险。

5.5.6 安全和隐私

区块链服务的安全和隐私需求宜包括：认证、授权、可获得、保密、不可抵赖、身份管理、完整性、审计、安全监控、事故反馈和安全策略管理。

区块链服务安全和隐私功能应包括：存取控制、保密、完整性和可获得性，保障数据存储、数据传输和数据应用等多个方面的安全和隐私。

5.5.7 经济合理

经济合理是指构建**区块链**系统时，在满足需求的前提下，技术选型应尽可能降低技术复杂度，规避高能耗的技术方案。

5.5.8 安全可信

安全可信是满足《中华人民共和国网络安全法》要求的一个重要方面。建设**区块链**系统，应积极贯彻落实国家网络安全和信息化战略部署，优先采用安全可信的软硬件产品。

6 功能视图

6.1 功能架构

区块链功能架构用一组高层的**功能组件**来描述**区块链**。**功能组件**代表了为执行第5章描述的与**区块链**相关的各种**角色**和**子角色**的**区块链活动**的功能集合。

功能架构通过分层框架来描述组件。在分层框架中，特定类型的功能被分组到各层中，相邻层次的组件之间通过接口交互。

6.1.1 分层框架

BRA功能架构的分层框架包括4层，以及一个跨越各层的跨层功能集合。这4层分别是：

a） 用户层；

b） 服务层；

c） 核心层；

d） 基础层。

跨越各层的功能称为跨层功能。

分层框架如图11所示。

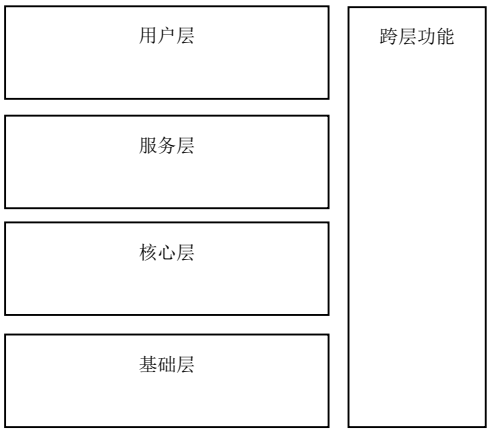


图11 区块链层次框架

框架中的每一层在后续章节中描述。

6.1.1.1 用户层

用户层是面向用户的入口。通过该入口，使用**区块链**服务的**区块链**服务客户和**区块链**服务提供方及其**区块链**服务进行交互，执行与客户相关的管理功能，维护和使用**区块链**服务。用户层也可将**区块链**服务输出到其他资源层，提供对跨层**区块链**服务的支持。

6.1.1.2 服务层

服务层为应用提供可靠高效的**区块链**访问和监控，即：

a） 通过调用核心层**功能组件**，提供统一接入和节点管理等服务；

b） 通过高效缓存、可靠存储、均衡负载等，为用户提供可靠高效的服务能力。

6.1.1.3 核心层

核心层是**区块链**系统的核心功能层。其中，节点间的共识机制，以及在此共识机制之上的数据与账本记录，奠定了**区块链**系统的根基；时序服务模块为**区块链**系统提供统一的时序；加密、摘要与数字签名等模块，保证了**区块链**系统的安全合规与防篡改；此外，根据应用场景的不同，可以有选择地添加能自动执行预设逻辑的智能合约。

核心层基于基础层提供的硬件或网络基础体系实现相应功能，并为服务层提供相关功能支持服务。

6.1.1.4 基础层

基础层提供了**区块链**系统正常运行所需要的运行环境和基础组件。这也是大多数软性系统运行所依赖的资源，如数据存储、运行容器、通信网络等。该层可视作**区块链**系统的基础支撑。

6.1.1.5 跨层功能

跨层功能提供跨越多个功能层次能力的**功能组件**。跨层功能可进行分组。

已定义的跨层功能子集包括：

a） 开发能力；

b） 运营能力；

c） 安全能力；

d） 监管和审计能力。

6.2 功能组件

本节从**区块链功能组件**通用集的角度描述了**区块链**架构。一个**功能组件**是 BRA 的一个功能元素，用来执行一个**活动**或**活动**的一部分。该**功能组件**在具体的参考架构实现中有相应的实现组件，例如:软件组件、子系统或应用。

图 12 展示了使用分层框架方式组织的对 BRA 组件的高层次概述。

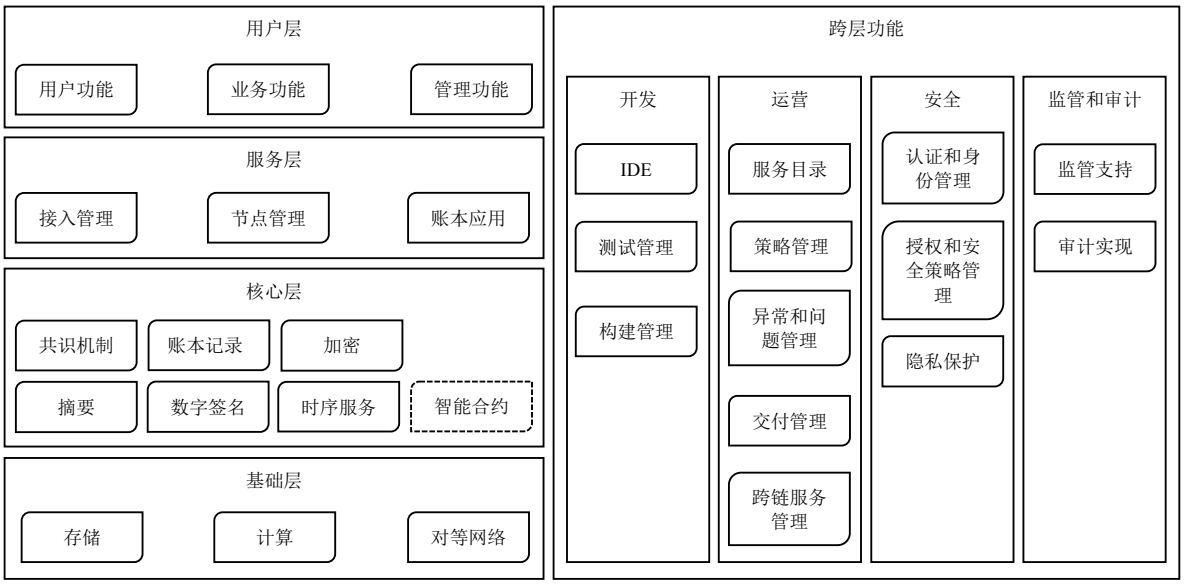


图12 区块链参考架构功能组件

6.2.1 用户层功能组件

用户层**功能组件**包括：

a） 用户功能；

b） 业务功能；

c） 管理功能。

提供给**区块链**服务客户的服务类型可以分为两大类：功能服务和自服务管理服务。后者可进一步分解为业务服务和管理服务。

提供给**区块链**服务客户的接口包括了**区块链**服务的主要功能，该接口不同于服务层所使用的接口，它将不同类型的功能封装成**区块链**服务。

6.2.1.1 用户功能

用户功能**功能组件**支持**区块链**服务客户访问和使用**区块链**服务（使用**区块链活动**）。在面向查询业务需求的场景下，用户功能**功能组件**可以运行在一个浏览器环境中，为**区块链**服务客户提供一个有组织的、架构化的**区块链**数据视图。在大部分的业务场景下，用户功能**功能组件**是一个运行着业务处理、应用、账本资源和相关基础设施的企业级的业务系统。

典型的用户功能**功能组件**应包含以下功能：

a） 用户界面：**区块链**服务客户与**区块链**服务进行交互的功能，可以是命令行界面或图形用户接口以及 API 等形式；

b） 事务提交：将**区块链**服务客户的特定事务请求（查询、更新）提交到**区块链**网络的功能。

6.2.1.2 业务功能

业务功能**功能组件**支持 BSC：**区块链**服务业务管理者的**活动**包括：**区块链**服务的选择和订购，使用**区块链**服务涉及的账务和财务管理，以及支持 BSC：**区块链**服务集成者的**活动**，包括跨链链接和**区块链**数据交换服务。**区块链**业务能力只能通过使用**区块链**服务来获取。

6.2.1.3 管理功能

管理功能**功能组件**支持 BSC：**区块链**服务管理者的**区块链活动**，包括成员管理服务、对服务**活动**和服务使用的监控、事件处理和问题报告、安全管理服务。**区块链**管理能力只能通过使用**区块链**服务来获取。

典型的管理功能**功能组件**应包含以下功能：

a） 成员管理服务：为**区块链**服务客户提供身份管理、权限管理、数据保密以及可审计的服务；

b） 监控管理：为**区块链**服务客户提供故障监测和**区块链**网络运行状态的监控服务；

c） 事件管理：为**区块链**服务客户提供预定义或自定义事件的服务；

d） 问题管理：为**区块链**服务客户提供**区块链**网络问题跟踪、报告的服务；

e） 安全管理：确保**区块链**服务客户账号安全性的服务。

6.2.2 服务层功能组件

服务层包含对用户层提供接入服务的实现。通过调用核心层**功能组件**，为用户层提供可靠接入服务支撑，需要满足功能操作的原子性和高性能。服务层**功能组件**至少包含对用户层提供接入服务访问接口，同时，应包含支持接口调用的开发工具包。

服务层**功能组件**应包括：

a） 接入管理；

b） 节点管理；

c） 账本应用。

6.2.2.1 接入管理

接入管理**功能组件**提供跨进程调用功能，为外部业务系统及用户层提供核心层接入服务。

接入管理**功能组件**应包括以下功能：

a） 账户信息查询：提供**区块链**服务客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**区块链**区块、事务详情等查询服务；

c） 事务操作处理：将**区块链**服务客户提交的特定事务操作请求提交到**区块链**网络。

宜包括：

a） 接口服务能力管理：支持接口调用频度设置和事务操作及账本查询缓存设置；

b） 接口访问权限管理：接口的访问权限等级通常分为低等级权限、中等级权限和高等级权限三类，针对不同的用户可以配置不同的访问权限。

6.2.2.2 节点管理

节点管理**功能组件**支持对**区块链**节点的信息查询和管理控制，**区块链**节点通常至少包括共识节点和接入节点两种。共识节点参与**区块链**网络共识过程，用于区块的生成。接入节点用于外部应用系统同步账本信息和提交事务处理。

节点管理**功能组件**应至少包括以下功能：

a） 节点服务器信息查询：提供**区块链**节点服务器的节点状态信息查询服务；

b） 节点服务启动关闭控制：提供**区块链**节点服务器的启动与关闭服务；

c） 节点服务配置：提供**区块链**节点服务器的节点服务能力配置；

d） 节点网络状态监控：提供**区块链**节点服务器网络连接状态监控服务；

e） 节点授权管理：提供**区块链**节点准入准出配置和节点事务处理及账本查询授权配置。

6.2.2.3 账本应用

账本应用**功能组件**通过调用核心层**功能组件**，实现基于**区块链**账本记录**功能组件**（见 6.2.3.2）的应用。一般应包括以下功能：

a） 链上内容发行和交换；

b） 共识前的逻辑验证和共识后的结果验算；

c） 可对特定事务处理进行多签名权限控制设置；

d） 可基于**智能合约功能组件**（见 6.2.3.8）执行合约逻辑。

6.2.3 核心层功能组件

核心层**功能组件**应包括：

a） 共识机制；

b） 账本记录；

c） 加密；

d） 摘要；

e） 数字签名；

f） 时序服务。

宜包括：**智能合约**。

6.2.3.1 共识机制

共识机制指**区块链**网络中各节点对在**区块链**系统中进行事务或状态的验证、记录、修改等行为达成一致确认的方法。在**区块链**系统中，根据不同的业务需求、**区块链**网络组织形式选择不同的适用**共识算法**来实现共识机制。

共识机制**功能组件**应具备以下功能：

a） 支持多个节点参与共识和确认；

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） 防止任何独立的共识节点未经其他共识节点确认而在**区块链**系统中进行信息记录或修改；

d） 应具备一定的容错性，包括节点物理或网络故障的非恶意错误，以及节点遭受非法控制的恶意

错误，以及节点产生不确定行为的不可控错误。

6.2.3.2 账本记录

账本记录泛指**区块链**中分布式数据的存储机制，通过不同节点对账本的共同记录与维护，形成**区块链**系统中数据的公共管理、防篡改、可信任的机制。账本记录**功能组件**应包括以下功能：

a） 支持持久化存储账本记录；
b） 支持多节点拥有完整的数据记录；
c） 支持向获得授权者提供真实的数据记录；
d） 确保有相同账本记录的各节点的数据一致性。

6.2.3.3 加密

加密功能组件是**区块链**底层安全机制的核心，一般具体包括**加密**和解密两个操作：**加密**操作是把明文数据转化为密文数据，解密操作是把密文数据还原为明文数据。根据**加密**密钥和解密密钥是否相同，**加密**算法分为对称**加密**算法和非对称**加密**算法。从适用场景来看，对称**加密**算法一般用于普通数据的**加密**，而非对称**加密**算法除了用于普通**加密**之外，还适用于密钥交换和**数字签名**等场景。

加密功能组件宜具备以下功能：

a） 支持国际主流**加密**算法，如 AES256 等对称**加密**算法和 RSA、ECC 等非对称**加密**算法；
b） 支持我国商密算法，如 SM4、SM7 等对称**加密**算法和 SM2、SM9 等非对称**加密**算法；
c） 应具备明确的密钥管理方案，确保**区块链**底层安全机制正常运行；
d） **加密**算法应具备抵御破解的能力，宜定期审核**加密**算法的安全性，必要时采用更高破解计算复杂性的**加密**算法。

6.2.3.4 摘要

摘要功能组件又称数字摘要功能，将任意长度的消息输入变成固定长度的短消息输出。摘要功能一般通过摘要函数（或称 Hash 函数）来实现，摘要功能的输出值被称为摘要值或者 Hash 值。摘要功能主要用在对数据的完整性提供保护，对于给定的数据明文和摘要，摘要功能可以验证该数据明文是否被篡改。

摘要功能组件宜具备以下功能：

a） 支持国际主流**摘要算法**，如 SHA256 等；
b） 支持我国商密算法，如 SM3 等；
c） **摘要算法**应具备抵御破解的能力，宜定期审核**摘要算法**的安全性，必要时采用更高破解计算复杂性的**摘要算法**。

6.2.3.5 数字签名

数字签名功能组件被接收者用以确认数据单元的完整性以及不可伪造性，即：确定消息确实是由签发方签署的。**数字签名**技术是非对称**加密**技术与数字摘要技术的结合，一般包括**数字签名**和签名验签两个具体操作。**数字签名**操作指签名者用私钥对信息原文进行处理生成**数字签名**值；签名验签操作指验证者利用签名者公开的公钥针对数字签名值和信息原文验证签名。

数字签名功能组件宜具备以下功能：

a） 支持国际主流的**数字签名**算法，如 RSA、ECC 等；
b） 支持我国商密的**数字签名**算法，如 SM2 等；
c） **数字签名**算法应具备抵御破解的能力，宜定期审核**数字签名**算法中使用的非对称**加密**算法和**摘要算法**的安全性，必要时采用更高破解计算复杂性的非对称**加密**算法和**摘要算法**；

d） 在部分应用场景下，也可引进权威公正的第三方 CA 机构签发的数字证书，来进行**数字签名**和签名验证相关工作，确保信息的机密性、完整性及不可抵赖性。

6.2.3.6 时序服务

对于**区块链**系统中的行为或数据需记录相应的一致性的时序，可以选择特定的时序机制或工具。**区块链**系统时序服务**功能组件**应具备以下功能：

a） 支持统一账本记录时序；

b） 具备时序容错性；

c） 必要时，支持集成可信第三方时序服务。

6.2.3.7 智能合约

根据应用场景的不同需求，**区块链**系统可有选择性地提供**智能合约**功能。通常情况下实现**智能合约**的**功能组件**应包括：

a） 开发运行环境，包括：

1） 提供编程语言支持，必要时可提供配套的集成开发环境；

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） 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内容升级；

3） 支持向账本中写入合约内容。

6.2.4 基础层功能组件

区块链基础层提供了**区块链**系统正常运行所需要的硬件设备之上的运行环境和基础组件。典型来说，基础层**功能组件**包括：

a） **对等网络**；

b） 存储；

c） 计算。

6.2.4.1 对等网络

区块链系统运行的底层拓扑结构是分布式**对等网络**，采用**对等网络**协议组织**区块链**中的各个网络节点。各个节点间通常使用点对点通信协议完成信息交换以支撑上层功能。

对等网络功能组件通常应具备以下功能：

a） 能够进行点对点之间的高效安全通信；

b） 能够提供点对点通信基础上的多播能力；

c） 应支持对节点的动态添加、减少的识别。

6.2.4.2 存储

存储**功能组件**提供**区块链**运行过程中产生的各种类型数据，如账本、交易信息等的写入及查询功能，相关选型包括但不限于关系型数据库、键值对数据库、文件数据库等。

存储**功能组件**通常应具备以下功能：

a） **对等网络**中，能够被每个节点部署并使用；

b） 能够高效、安全、稳定地提供数据写入及查询服务。

对于采取分库分表的数据存储方案，存储**功能组件**还应包括数据的分片及路由处理能力。

6.2.4.3 计算

计算**功能组件**提供**区块链**系统运行中的计算能力支持，包括但不限于容器技术、虚拟机技术、云计算技术等。一般应具备以下功能：

a） 对**区块链**系统提供运行环境支持；

b） **对等网络**中，能够被每个节点采用。

6.2.5 跨层功能

6.2.5.1 开发功能组件

开发**功能组件**支撑**区块链**服务开发方的**活动**，包括服务实现的开发、构建管理和测试管理。

开发**功能组件**由以下组件构成：

a） IDE；

b） 构建管理；

c） 测试管理。

6.2.5.1.1 IDE

IDE **功能组件**提供用于**区块链**及相关应用的开发，支持模块的开发，提供服务组合的工具。

IDE **功能组件**支持使用**区块链**服务提供方所提供的服务能力，包括统一接入、节点管理及时序服务，并能使用服务的核心层，以及访问服务的基础层。

IDE **功能组件**支持开发服务相关的配置元数据的生成；支持供服务提供商运营系统使用的服务配置脚本和组件的编写或生成。

6.2.5.1.2 构建管理

构建管理**功能组件**构建可发布的软件包。该软件包可提交给**区块链**服务提供方，并部署在生产环境。软件包既包含用于服务实现的软件，又包含配置元数据和配置脚本。

构建管理功能包括：

a） 支持自动化构建软件包功能；

b） 提供自动化编译功能；

c） 在构建过程中出错时，提供出错信息；

d） 实现构建过程的审核流程；

e） 构建系统提供多语言支持；

f） 构建系统提供多平台支持。

6.2.5.1.3 测试管理

测试管理**功能组件**支持对**区块链**所有的服务进行测试。测试管理组件应能生成测试报告，并将测试报告和服务实现软件一同提供给服务提供者。

一般情况下，测试在一个特殊的独立的测试环境中执行。独立的测试环境应是对生产环境的仿真。在不影响生产环境的情况下，测试工作也可在生产环境中进行。测试环境应由**区块链**服务提供方或者**区块链**服务关联方提供。

测试管理**功能组件**应至少包括以下功能：

a） 测试管理组件应支持测试计划、测试方案、测试报告、测试用例等内容的管理；
b） 支持自动生成测试报告；
c） 测试环境与生产环境集成的情况下进行测试不应影响生产环境；
d） 宜支持测试过程自动化；
e） 提供测试用例库、测试数据库管理功能。

6.2.5.2 运营功能组件

运营**功能组件**包括一组与操作有关的管理功能，这些功能用于管理和控制提供给用户使用的**区块链**服务。

运营**功能组件**包括：

a） 服务目录；
b） 策略管理；
c） 异常和问题管理；
d） 交付管理；
e） 跨链服务管理。

6.2.5.2.1 服务目录

服务目录功能提供某一特定**区块链**服务提供方的所有**区块链**服务列表。服务列表包括/参考所有部署、提供和运行**区块链**服务有关的技术信息。

6.2.5.2.2 策略管理

策略管理功能提供**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。这些策略包括用于**区块链**服务本身及其使用的业务、技术、安全、隐私和认证等策略。

6.2.5.2.3 异常问题管理

异常问题管理功能提供事故和问题报告的捕获能力，并通过分析来管理这些报告。

事故和问题可由**区块链**服务提供方系统或**区块链**服务用户检测和报告。

6.2.5.2.4 交付管理

交付管理功能提供**区块链**服务交付的管理功能，以服务实现和访问端点两种形式提供。同时，该功能提供必需的工作流，以确保这些服务元素以正确的顺序提供。

6.2.5.2.5 跨链服务管理

跨链服务管理功能提供服务提供方的运营系统、业务系统和跨链服务提供方（见附录B）的管理及业务功能的连接功能。跨链服务**功能组件**负责根据请求建立与跨链服务提供者的连接，传送相关的身份和认证信息。

6.2.5.3 安全层功能组件

安全层的功能主要为**区块链**各**功能组件**层以及层间的协议提供保密性、完整性、可用性和隐私保护等安全属性的保障。这些安全功能广泛用在了用户和节点身份认证、交易协议设计、链式数据组织、通讯信道**加密**和应用数据访问控制之中。

安全层应至少包括以下功能：

a） 认证和身份管理；
b） 授权和安全策略管理；

c） 隐私保护。

6.2.5.3.1 认证和身份管理

认证和身份管理功能提供用户的身份确认过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使**区块链**系统访问控制策略能够可靠、有效地执行。认证和身份管理**功能组件**包括以下功能：

a） 支持建立身份管理的策略，确立认证基于用户知道的信息、用户拥有的信息还是用户独一无二的身体特征；

b） 支持利用具体身份认证方法支撑身份管理策略；

c） 支持在身份认证的基础上建立用户身份管理机制。

6.2.5.3.2 授权和安全策略管理

授权和安全策略管理功能提供授与用户访问或者使用某种资源的权限，以及制定在某个安全区域内所有安全相关**活动**必须遵循的一套规则的功能。授权和安全策略管理**功能组件**包括：

a） 授权用户访问和使用资源权限的功能；

b） 设置授权和安全规则的功能；

c） 授权和安全规则由安全权力机构控制的功能。

6.2.5.3.3 隐私保护

隐私保护**功能组件**主要是保护**区块链**应用中用户身份和事务处理等敏感信息不被泄露或非法获取，这些信息只有通过充分授权才能被访问。

隐私保护功能通常通过数据**加密**和访问控制手段来实现，通常有以下四个隐私保护策略：

a） 由认证机构代理用户在**区块链**上进行事务处理，用户资料和个人行为不进入**区块链**；

b） 不采用全网广播方式，而是将数据的传输限制在正在相关的授权节点之间；

c） 对用户数据的访问采用权限控制，持有密钥的访问者才能解密和访问数据；

d） 采用例如零知识证明、环签名和同态**加密**等隐私保护算法，规避隐私暴露。

隐私保护**功能组件**宜具有以下功能：

a） 支持通过认证机构代理用户在**区块链**上进行事务处理；

b） 支持将数据的传输限制在特定授权节点间；

c） 支持用加解密方法对用户数据的访问采用权限控制；

d） 支持对事务发起方/接收方的信息及事务信息本身进行信息隐藏。

6.2.5.4 监管和审计功能组件

监管和审计**功能组件**根据**区块链**服务关联方的治理要求使**区块链**服务符合可监管与可审计的特性，避免**区块链**网络游离于法律法规以及行业规则之外，成为洗钱、非法融资或犯罪交易的载体。应至少包括以下功能：

a） 监管支持；

b） 审计实现。

6.2.5.4.1 监管支持

监管支持功能，主要用于满足监管机构对于**区块链**服务的环境、系统、可用性、灾备、系统运维、所支持业务的合规性等方面的规定，根据行业监管机构与监管方式的不同，所涉及的功能的深度与广度亦不同。具体要求包括：

a） 应具备完善健全的监管治理体系。通过事前准入控制、事中权限控制、事后追溯等技术手段实

现监管目标，保证记录不可篡改、可追溯与可稽核；

b） 宜实现监管机构加入**区块链**网络作为其中一个节点进行即时监管。监管节点可对数据完整性、有效性和流程合规性进行即时的监督与稽核，并对异动交易进行干预，封停有非法行为的业务；监管干预**活动**相关的数据和证据应进行完整记录和保存；

c） 设置明确的监管治理规则。应同时支持由人参与监督管理的、无法用技术自动实现的规则，由组织机构或管理人员依据法律、行政法规、部门规章等进行监管治理的规则，并鼓励充分利用**智能合约**等技术有效支持智能化的监管操作，提供可自动化实现的监管规则；

d） 保存与服务、资源、性能相关的数据和证据。这些数据和证据包括协议所有相关方的**活动**和运营环境条件的记录和日志，需要以安全的方式收集和维护。

6.2.5.4.2 审计实现

审计实现功能，主要用于实现**区块链**网络的审计内控、责任鉴定和事件追溯等方面的要求，需要以有效的技术手段，配合业务所属的行业标准进行精确的审计管理，具体要求包括：

a） 宜对**区块链活动**的事前、事中、事后三个阶段进行审计，建立包含查处违规违纪审计、内控制度审计、绩效审计等内容的审计指标；

b） 宜实现**区块链**服务审计方加入**区块链**网络作为其中一个节点进行实时审计，或允许**区块链**服务审计方作为**区块链**网络之外的第三方机构，按需或定时获得**区块链**网络中的数据与证据。鼓励基于**区块链**技术的不可篡改和可追溯特点，实时核查审计被审计对象的全部记录并作为审计证据；

c） 宜实现**区块链**网络与其他相关系统的对接与交互，提高审计效率和审计结果的可靠性；

d） 保存与审计**活动**相关的数据和证据。数据和证据包括但不限于**区块链**所有相关方的**活动**和运营环境条件的记录和日志、审计员的审计查看动作记录、审计过程和结果信息等，应避免审计信息的泄漏。

7 用户视图和功能视图之间的关系

7.1 概述

在第 5 章介绍**区块链角色**与**活动**的用户视图，第 6 章介绍包含**功能组件**的功能视图的基础上，本章描述**角色**和**活动**与**功能组件**之间的逻辑映射关系。

映射关系是标准的一部分。标准中的映射关系可应用于：

a） 明确信息流或其他类型**互操作**的程度；

b） 确保制定的质量（例如安全或服务水平）。

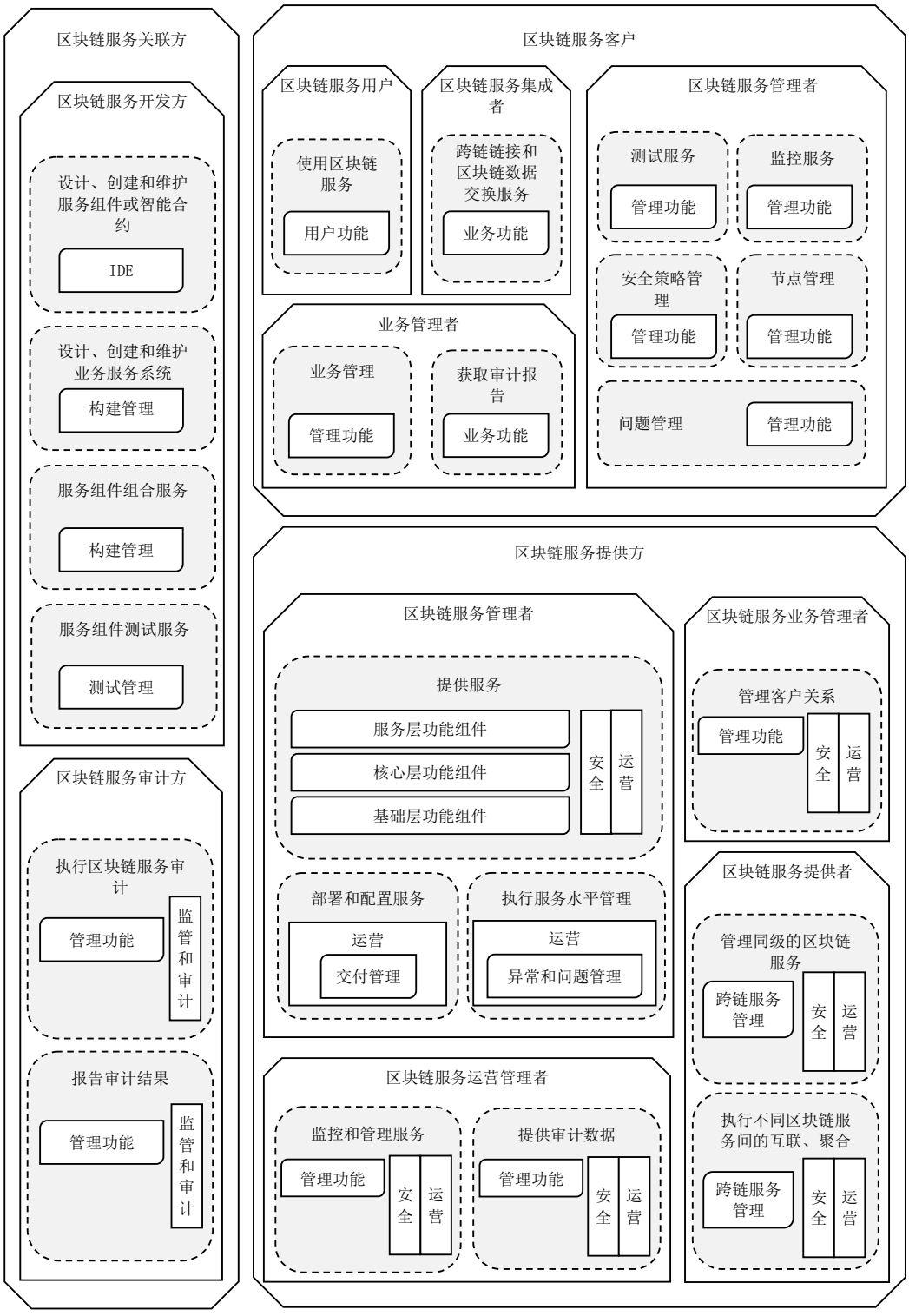
本架构中定义的逻辑关系是确定 BRA 及其行为的重要组成部分。该逻辑关系描述内容包括 BRA 组件间交互所需的信息流。

7.2 关系

图13展示了BLDT-RA主要元素的常用配置，包括**角色**、**区块链活动**和组件。

在图13中，**角色**、**子角色**、**功能组件**的图例与图1中展示的相同。此外，**区块链活动**用圆角虚线填充矩形表示。从图13中可以明显看出：**角色**是**区块链**服务**活动**的集合，**区块链**服务**活动**本身又通过组件实现。

共同关注点包括**模块化**，性能，**互操作**，数据一致性，安全和隐私，经济合理，安全可信等。共同关注点在图13中最外层的边框内标识，表明共同关注点的内容适用于图13中所有其他元素，包括**角色**、**活动**和组件。



模块化，性能，互操作，数据一致性，安全和隐私，经济合理，安全可信

图13　角色、区块链活动和组件的通用视图

附 录 A
（规范性附录）
区块链和分布式账本技术概览

A.1 区块链关键特征

本条标识并描述**区块链**关键特征。本条无意于限制任何具体的部署方法、服务交付方法或业务运营方法。

区块链关键特征包括：

——分布式对等。**区块链**利用**对等网络**模型，对各参与节点进行组网，并在各对等节点间分配任务和共享资源。网络节点间无需依赖中心节点即可实现信息共享和交换。对等节点既可以是资源、服务和内容的提供者，也可以是获取者，从而降低了组网复杂度并提高了网络系统的容错性。

——数据块链式。**区块链**网络中通过对某一时间段内发生的事务数据进行验证、打包和共识，形成数据区块，同时每一个区块与上一个区块通过密码学特征的方式有序链接。

——不可伪造和防篡改。向**区块链**写入数据的事务请求需附有发起方私钥签名，该签名随事务请求在网络参与节点间广播并进行验证，因此事务请求是不可伪造和防篡改的。同时，块链式数据结构进一步保证了防篡改性。

——透明可信。**区块链**中信息的传递和区块的生成都遵循透明的共识规则；每一次事务处理都以特定的形式发送给其他节点，授权节点可以保存与其权限相关的历史记录，保证了链上数据的透明性。每一次事务处理和区块的生成均可以由授权节点根据既定规则验证其合法性，并通过共识机制进行记录，保证了记录结果的可信。

——高可靠性。**区块链**作为典型的分布式应用，多个节点拥有完整的服务能力及全量数据，部分节点的异常或者恶意行为不会影响整体服务的可用性和连续性，以及数据的完整性和真实性。

A.2 区块链服务能力类型和区块链服务类别

具有为**区块链**服务客户按需提供**区块链**功能的能力，在提供服务过程中，**区块链**服务提供方提供**区块链**的安装和管理等。

——基础设施能力类型。**区块链**服务客户能配置和使用**对等网络**上的计算、存储、网络和平台资源的一类**区块链**能力类型。

——数据能力类型。**区块链**服务客户能使用**区块链**服务提供方的数据工具，管理、查询和分析客户数据的一类**区块链**能力类型。包括但不限于数据开放和共享能力、数据所有权管理能力、数据迁移和备份恢复能力、跨链数据交互能力以及与大数据的集成能力。

——应用能力类型。**区块链**服务客户能使用**区块链**服务提供方的应用的**区块链**能力类型。除**区块链**软件即服务能力以外，典型的还包括交互与协作能力、审计即服务能力、身份认证即服务能力、管理即服务能力、安全即服务能力、财务即服务能力等专业化的服务能力。

典型的**区块链**服务类别包括：

——基础设施即服务
——**区块链**软件即服务
——审计即服务
——身份认证即服务
——管理即服务
——安全即服务
——财务即服务

注：除了本标准列举的各种**区块链**服务类别外，还可能有其他服务类别存在或出现。

表A.1 区块链服务类别和区块链服务能力类型

区块链服务类别	区块链服务能力类型		
	基础设施	数据	应用
基础设施即服务	○		
区块链软件即服务			○
审计即服务		○	○
身份认证即服务		○	○
管理即服务			○
安全即服务			○
财务即服务		○	○

A.3 区块链部署模式

区块链部署模型是指根据不同应用场景和设计体系，采用不同的开放共享和节点权限方案对**区块链**进行组织的方式。其中：

区块链部署模型包括：

——公有链。任意**区块链**服务客户均可使用，任意节点均可接入，所有接入节点均可参与共识和读写数据的一类**区块链**部署模型。

——联盟链。仅由一组具有利益相关的特定**区块链**服务客户使用，仅有授权节点可接入，接入节点可按规则参与共识和读写数据的一类**区块链**部署模型。

——专有链。仅由单个**区块链**服务客户使用，仅有授权的该客户节点可接入，接入节点可按规则参与共识和读写数据的一类**区块链**部署模型。

A.4 区块链和分布式账本技术的关系

严格意义上讲，**区块链**和**分布式账本技术**这两个概念的原始内涵具有明显差异。**区块链**的基本技术特征是：将一段时间内发生的事务处理编组成区块，区块之间以密码学特征（例如 Hash 值）方式按先后顺序链接起来，形成以区块为基本单元的“链”，并且将该“链”在**区块链**网络参与节点间复制和共享，同时链上内容依据不同的共识机制由参与节点组成的网络集体维护。而**分布式账本技术**是一类用来实现**分布式账本**的技术，强调的是事务处理通过复制和共享的账本来实现，并且该账本由所在网络的参与者进行校验及维护，并不指定具体的技术特征。

在很多应用场景中，**区块链**和**分布式账本技术**具有密不可分的联系。**区块链**是实现**分布式账本**的一种常用的技术手段，某种程度上可以将**区块链**看作是**分布式账本技术**的一种。尤其是在不同的利益、关注点和需求的驱使下，两者的应用实践逐渐体现了一种相互融合的趋势。因此，**区块链**和**分布式账本技术**被同时提出来，主要是用于描述符合两者共同点的技术统称。

附 录 B
（资料性附录）
用户视图和功能视图说明

本附录对用户视图和功能视图间的关系提供进一步描述。

B.1 区块链服务客户和提供方之间的关系

在**区块链**服务客户和**区块链**服务提供方关系中有三个关键要素：

a） BSC：**区块链**服务客户使用**区块链**服务提供方的**区块链**服务来实现自身的业务目标；

b） BSC：**区块链**服务业务管理者基于**区块链**服务提供方的业务能力管理**区块链**服务并获取面向**区块链**服务监管方的报告；

c） BSC：**区块链**服务管理者基于**区块链**服务提供方提供的管理能力，从**区块链**服务客户的视角来管理**区块链**服务的使用。

B.1.1 功能关系

区块链服务客户通过用户功能**功能组件**提供的接口来使用**区块链**服务。接口根据面向的**区块链**服务需求的不同，提供定制化的**区块链**服务，但是服务接口需满足通用**区块链**服务需求，主要是识别**区块链**服务客户和验证**区块链**服务客户的需求。

BSC：**区块链**服务客户通过用户**功能组件**来执行使用**区块链**服务的**活动**，该**功能组件**通过统一接入**功能组件**来调用**区块链**服务。用户功能**功能组件**执行对 BSC：**区块链**服务客户的身份验证，并通过接入管理服务进行使用特定**区块链**服务能力的授权。如果被授权，接入管理**功能组件**即可调用各种业务**功能组件**实现**区块链**服务客户业务请求。

B.1.2 业务关系

BSC：**区块链**服务业务管理者通过用户层的业务功能**功能组件**来完成各类**区块链活动**：选择和购买服务、执行业务管理和获取审计报告。业务功能**功能组件**通过统一接入**功能组件**来调用**区块链**服务提供方的业务能力。

用户功能**功能组件**验证 BSP：**区块链**服务业务管理者的身份，并授权其访问业务能力的特定功能。业务功能**功能组件**与管理功能**功能组件**交互来完成 BSC：**区块链**服务业务管理者的各类请求。

B.1.3 管理关系

BSC：**区块链**服务管理者通过管理功能**功能组件**执行以下**区块链活动**：

a） 成员管理服务；

b） 监控管理；

c） 事件管理；

d） 问题管理；

e） 安全管理。

管理功能**功能组件**通过用户功能**功能组件**的接口来调用**区块链**服务提供方的管理功能能力组件。用户功能**功能组件**完成对 BSC：**区块链**服务管理者的身份验证并授权其使用特定管理**功能组件**的功能。管理**功能组件**与用户功能**功能组件**一起响应 BSC：**区块链**服务管理者的请求。

用户功能**功能组件**验证 BSP：**区块链**服务管理者的身份，并授权其访问管理功能**功能组件**的特定功能。管理功能**功能组件**与用户功能**功能组件**交互来完成 BSC：**区块链**服务管理者的各类请求。

其他与**区块链**服务客户和**区块链**服务提供者之间关系相关的因素能包括客户和提供者之间的协议。该协议能包含 SLA、知识产权和管理，例如对个人数据的保护、访问控制。

B.2 提供方和跨链提供方之间的关系

一个**区块链**服务提供方能够使用其他**区块链**服务提供方提供的一个或多个**区块链**服务，并将这一个或多个**区块链**服务进行封装和加工形成新的**区块链**服务进行提供。这样的**区块链**服务提供方可称为跨链服务提供方。

区块链服务提供方与**区块链**跨链服务提供方之间的关系包含两个**功能组件**：

a） 跨链**区块链**服务提供方使用其他**区块链**服务提供方的**区块链**服务；

b） 跨链**区块链**服务管理者通过使用其他**区块链**服务提供方的业务能力和管理能力来使用和控制其他**区块链**服务提供方的**区块链**服务。

对于跨链**区块链**服务提供方来说，其承担**区块链**服务客户的**角色**。其他**区块链**服务提供方的服务提供给跨链**区块链**服务提供方使用。同时，跨链**区块链**服务提供方通过其他**区块链**服务提供方和**区块链**服务客户联系起来时，需要特别考虑安全、容量、性能等方面。

跨链**区块链**服务提供方需要确保其他**区块链**服务提供方的服务 SLA 满足自身提供的服务要求，并且任何违背 SLA 的情况都得到适当处理。

跨链**区块链**服务提供方和**区块链**服务提供方关系中包含三类接口：管理接口、业务接口和服务接口，这些接口提供了与**区块链**服务客户和**区块链**服务提供方间接口大体相同的能力。

B.3 区块链服务开发方和提供方之间的关系

区块链服务开发有两类，**区块链**系统中组件功能的服务开发和基于**区块链**系统的业务系统的开发，他们与**区块链**服务提供方的关系如下描述。

B.3.1 区块链组件功能的服务开发方与区块链服务提供方之间的关系

区块链服务组件开发者完成服务功能实现，将服务功能发送部署到**区块链**网络的节点中，通过**区块链**服务提供方提供的运行环境进行运维与调用支持，因此**区块链**组件服务开发者与**区块链**服务提供方交互实现以下目标：

a） 检查**区块链**服务提供方的服务功能执行环境；

b） 测试服务实现；

c） 提交部署服务功能实现代码；

d） 提供**区块链**服务组件的维护与扩展。

开发**区块链功能组件**服务开发者**活动**包括：服务组件开发服务、测试服务和维持服务。这些**活动**依赖**区块链**开发环境、部署管理、接口管理和测试管理等**区块链**系统组件。

区块链组件服务开发者使用**区块链**服务提供方支持的开发语言实现组件服务功能，然后使用**区块链**服务部署管理部署服务和相关的组件。**区块链**服务提供方对提交部署的服务组件进行相关审核、验证或测试，通过**区块链**系统的事务提交共识后将服务组件部署到**区块链**网络中。

为了在目标执行环境运行服务实现和服务访问，安全、监控、管理、和自动化等需要正常启动，同样需要成功地集成到服务集成环境。**区块链**服务组件开发者部署地址与接口。此外认证和身份管理及授权和服务政策管理的信息和需求通过**区块链**服务提供方提供的**区块链**系统机制与服务组件集成。**区块链**服务管理者执行部署服务组件**活动**，结果是在提供服务**活动**中服务对用户是可用的。

B.3.2 基于区块链系统的业务应用开发方与区块链服务提供方之间的关系

基于**区块链**系统的业务应用开发方完成基于业务需求的相关业务应用功能，通过**区块链**服务提供方提供的**区块链**系统的接口服务与**区块链**系统进行集成，并在业务应用与**区块链**系统账本间实现数据的交互，以达成具体的业务应用目标，因此基于**区块链**系统的业务应用开发方与**区块链**服务提供方交互实现以下目标：

a） 使用并验证**区块链**服务提供方的应用接口服务；

b） 对**区块链**服务提供方的应用接口服务提出扩展或定制化需求；

c） 实现**区块链**系统与业务应用系统的集成；

d） 提供基于**区块链**系统的业务应用的维护与扩展；

e） 合作进行**区块链**系统与业务应用系统的联合运维。

基于**区块链**系统的业务应用开发方**活动**包括：基于**区块链**系统的业务应用开发服务、测试服务和维持服务。这些**活动**依赖**区块链**系统的接口服务环境、集成部署管理、接口管理和测试管理等**区块链**系统服务。

基于**区块链**系统的业务应用开发方使用**区块链**服务提供方提供实现组件服务功能，然后对**区块链**系统接口进行相关的测试与验证，并可根据特定业务需求向**区块链**服务提供方提出接口扩展或修订需求。在接口的使用规则上应做到双方协商一致，并形成接口设计规范。

在业务应用开发完成后，基于**区块链**系统的业务应用开发方应与**区块链**服务提供方共同进行**区块链**系统和业务系统的集成部署，并制定联合部署与运维的计划方案。算法宜制定一致的 SLA 服务标准与机制。

为了支持业务应用系统的运行，**区块链**服务提供方提供的**区块链**系统中的接口、安全、监控、管理、和自动化等需要正常启动，同样需要成功地集成到服务集成环境。此外在业务系统使用**区块链**系统的应用接口服务时，相关认证和身份管理及授权和服务政策管理的信息和需求通过**区块链**服务提供方提供的**区块链**系统机制与应用系统集成。

B.4 区块链服务提供方和审计方之间的关系

区块链服务审计方应审计议定的技术参数、政策及协议。

审计技术参数、政策及协议或由**区块链**服务提供方设定标准，或由审计者设定标准，或根据法律需要设定，选取哪个取决于审计结果的目标。

区块链服务审计方的审计内容有安全审计，隐私审计和性能审计。针对不同**区块链活动**，**区块链**服务审计方可通过**区块链**服务提供方的一组接口以程序调用方式获取审计证据，也可通过成为**区块链**网络中的审计节点直接获取审计凭证。审计凭证的格式将取决于审计标准与业务类型，凭证可以是程序文件的形式，也可以是日志记录。

B.4.1 安全审计

系统安全审计有各种各样的标准。涵盖信息安全管理的 ISO/IEC 27001 是其中之一。同时还有很多其他组织为**区块链**安全提供审计标准。

B.4.2 隐私审计

个人信息的保护是管理和或立法的典型对象，各种数据保护部门发布了各种程序、政策或系统的隐私安全的评定和或审计的指导方针。但**区块链**服务消费者可能与**区块链**服务提供方在不同的法律管辖范围，情况会变得更加复杂。数据审计者应按照数据保护部门的执导方针和相关标准，对**区块链**服务的隐私方面和**区块链**服务提供方针对隐私规则的操作进行评估。

B.4.3 性能审计

性能审计用于评估**区块链**服务提供方的能力是否与**区块链**服务性能目标一致，性能目标通常记录在 SLA 中。

B.5 区块链服务提供方和监管方之间的关系

区块链服务监管方依照法律、行政法规，制定并发布对**区块链**服务提供方及其**活动**进行监督管理的规章规则。

区块链服务监管方与**区块链**服务提供方的关系型**活动**有审批和报备、监管与处置、共同建立突发事件应急管理制度。

B.5.1 审批和报备

区块链服务提供方需遵从**区块链**服务监管方所制定的规章规则，**区块链**服务提供方的相关业务资质、业务范围、业务品种、风险状况、诚信状况、从业人员资质等需通过**区块链**服务监管方的审批和报备。

B.5.2 监管与处置

区块链服务监管方应对**区块链**服务提供方的业务**活动**及其风险状，进行非现场和现场监管，分析、评价**区块链**风险状况，**区块链**服务提供方违反规则的，**区块链**服务监管方应责令限期改正；逾期未改正的，或者其行为严重危及**区块链**服务提供方的稳健运行、损害其他**区块链**服务提供方或客户合法权益的，**区块链**服务监管方可以区别情形，采取暂停部分业务、停止批准开办新业务、终止业务等措施。

B.5.3 共同建立突发事件应急管理制度

区块链服务监管方应会同**区块链**服务提供方及有关部门建立突发事件应急管理制度，制定**区块链**突发事件处置预案，明确处置机构和人员及其职责、处置措施和处置程序，及时、有效地处置**区块链**突发事件。

参考文献

本附录不是本标准的有机组成。

[1] ISO/IEC/IEEE 42010:2011, Systems and software engineering—Architecture description

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