

# 中华人民共和国国家标准

GB/T 43582—2023

## 区块链和分布式记账技术 应用程序接口 中间件技术指南

Blockchain and distributed ledger technology—  
Application interface—Technical guidelines of middleware

国家标准全文公开系统专用，此文本仅供个人学习、研究之用，  
未经授权，禁止复制、发行、汇编、翻译或网络传播等，侵权必究。  
国家标准信息公共服务平台：<https://std.samr.gov.cn>

2023-12-28 发布

2024-04-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会



目 次

前言 ..... III

引言 ..... IV

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 技术架构 ..... 2

6 非功能性指南 ..... 7

附录 A（资料性） 区块链中间件接口描述参考 ..... 8

附录 B（资料性） 区块链中间件应用方法 ..... 9

参考文献 ..... 12





# 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。

本文件由中华人民共和国工业和信息化部提出。

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)归口。

本文件起草单位：厦门安妮股份有限公司、蚂蚁区块链科技(上海)有限公司、深圳市前海智慧版权创新发展研究院、中国电子技术标准化研究院、北京版全家科技发展有限公司、深圳前海微众银行股份有限公司、深圳市腾讯计算机系统有限公司、华为云计算技术有限公司、杭州趣链科技有限公司、上海万向区块链股份公司、永旗控股(北京)有限公司、北京百度网讯科技有限公司、京东科技信息技术有限公司、众安信息技术服务有限公司、国网区块链科技(北京)有限公司、工业和信息化部电子第五研究所、上海分布信息科技有限公司、四川长虹电器股份有限公司、南京鑫智链科技信息有限公司、复旦大学、中国科学院信息工程研究所、江苏恒为信息科技有限公司、北京大数据先进技术研究院、腾讯云计算(北京)有限责任公司、华为技术有限公司、蚂蚁科技集团股份有限公司、上海树图区块链研究院、北京微芯区块链与边缘计算研究院、上海零数众合信息科技有限公司、广州南方投资集团有限公司、上海阵方科技有限公司、湖南天河国云科技有限公司、北京中科金财科技股份有限公司、中国民航信息网络股份有限公司、上海奥若拉信息科技集团有限公司、达闼机器人股份有限公司、工银科技有限公司、浙商银行股份有限公司、联通数字科技有限公司、清雁科技(北京)有限公司、北京安妮全版权科技发展有限公司、香港理工大学、中央财经大学、北京信息科技大学、深圳市前海服务集团有限公司、深圳职业技术学院、敏于行(北京)科技有限公司、深圳市金融区块链发展促进会、深圳博思互联科技有限公司、法诺信息产业有限公司、北京中宏安科技发展有限公司、江西开创数码科技有限公司。

本文件主要起草人：郝汉、李鸣、昌文婷、张杰、胡怀勇、李斌、周平、李克鹏、张子怡、于秀明、李伟、杜宇、肖伟、王义、王栋、相里朋、笪鸿飞、李努锲、陶立春、阚海斌、张潇丹、张何东、刘天成、王保春、邵兵、张亮亮、余珊、任常锐、兰春嘉、劳卫伦、龚自洪、欧昀、宋文鹏、杨征、朱烨东、晏海水、谢辉、王绍刚、杨国正、阮建勇、赵伟、王理、郝佳诺、朱建明、倪渊、王永祥、王荆楠、蔡曜宜、孙林、姚辉亚、张凯文、康信伟、王晨辉、卢修禄、高玉翔、陈晓丰、郝玉琨、曹建农、王子博、荆博、王海龙、李达、邓鹤、肇雨濛、包小敏、陈若禹、崔春生、杜娟、杨珍、罗朗、姚驰、秦日臻、臧铖、刘齐军、张雁、刘冕宸、周子茗、汤智林、朱家彬、张瀚元、华崇鑫。

# 引 言

“十四五”规划纲要已将区块链列为七大新兴数字产业之一，明确提出了区块链技术创新、应用发展、监管机制完善的三大重点任务。目前，各行各业都在加快区块链基础设施建设与应用布局，已延伸至金融、物联网、智能制造、供应链管理、公共服务等多个领域。同时，区块链作为新兴技术也存在着底层技术不统一、开发与运用门槛高、缺乏高效的监管工具以及数据孤岛等问题。

本文件通过制定区块链中间件技术指南，为区块链中间件系统的开发提供指导，规范基于区块链技术的业务应用建设过程，有助于提高区块链应用服务质量、促进数据共享、提升产业协同能力，从而推动区块链技术赋能实体经济，成为数字时代的信任基石。



# 区块链和分布式记账技术 应用程序接口 中间件技术指南

## 1 范围



本文件确立了区块链中间件的技术架构和非功能性要素,提供了区块链中间件的技术指南。

本文件适用于:

- a) 指导区块链中间件系统的开发;
- b) 规范基于区块链中间件技术的业务应用建设过程;
- c) 为区块链中间件系统评测和技术选型提供参考。

## 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 32399—2015 信息技术 云计算 参考架构
- GB/T 33847—2017 信息技术 中间件术语
- GB/T 43572—2023 区块链和分布式记账技术 术语

## 3 术语和定义

GB/T 32399—2015、GB/T 33847—2017、GB/T 43572—2023 界定的以及下列术语和定义适用于本文件。

### 3.1

**区块链 blockchain**

使用密码链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源:GB/T 43572—2023,3.6]

### 3.2

**中间件 middleware**

位于系统软件之上,用于支持分布式应用软件,连接不同软件实体的支撑软件。

[来源:GB/T 33847—2017,2.1]

### 3.3

**智能合约 smart contract**

存储在分布式记账技术系统中的计算机程序,该程序的任何执行结果都记录在分布式账本中。

[来源:GB/T 43572—2023,3.72]

### 3.4

**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]

3.5

**角色 role**

一组服务于共同目的的活动的集合。

[来源:GB/T 32399—2015,3.2.7]

4 缩略语

下列缩略语适用于本文件。

API:应用程序接口(Application Programming Interface)

CA:证书授权(Certificate Authority)

IP:网际互连协议(Internet Protocol)

QPS:每秒查询率(Query Per Second)

TPS:每秒处理事务数(Transaction Per Second)

URL:统一资源定位符(Uniform Resource Location)

5 技术架构

5.1 总体架构

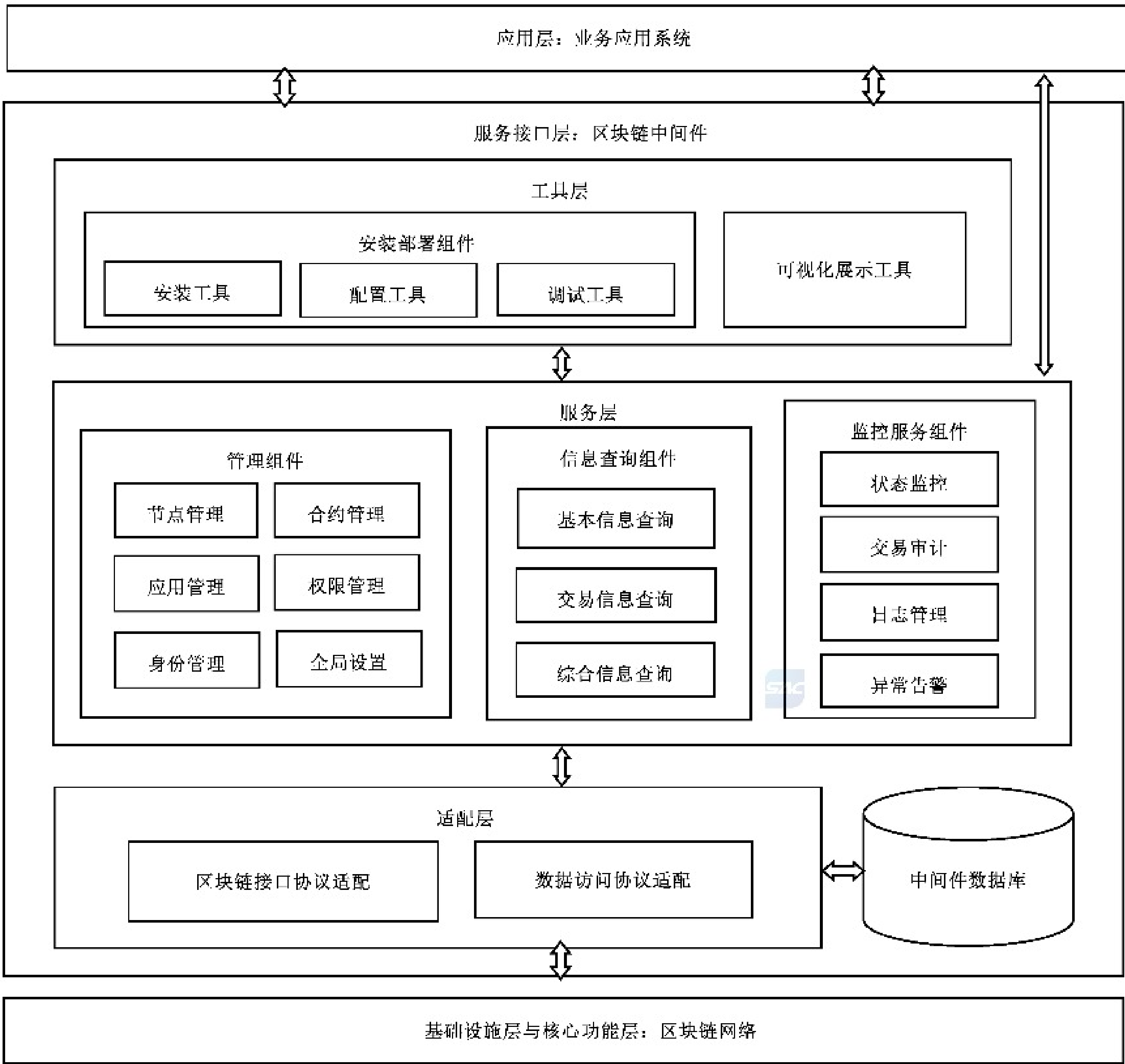
区块链中间件属于区块链系统架构的服务接口层,位于应用层和基础设施层与核心功能层之间,为应用层的业务应用系统提供统一的工具、组件与服务,并简化业务应用系统对区块链网络的访问和操作。

区块链中间件包括适配层、服务层、工具层,各层的功能组件构成如下。

- a) 适配层具备中间件数据库,提供链上系统数据和业务数据索引、缓存和关联等能力;中间件产生的数据保存在中间件数据库中。
- b) 适配层具备对不同数据访问协议的适配,以屏蔽不同数据库之间的差异,提供统一的接口对数据进行访问与操作。
- c) 服务层具备管理、信息查询、监控服务等组件:
  - 1) 管理组件提供管理节点、账户、证书、私钥、应用接入、智能合约等功能;
  - 2) 信息查询组件提供数据信息检索和查询的功能;
  - 3) 监控服务组件提供监控区块链节点状态、服务器资源、中间件接口调用信息、交易异常信息、系统错误日志信息、操作记录、异常告警等功能。
- d) 服务层具备对不同区块链网络接口协议的适配,通过对区块链网络核心功能层功能组件的封装,为业务应用系统提供统一的、与区块链进行交互的接口组件,涵盖合约的验证、部署、交易发送、信息查询等。
- e) 工具层具备安装部署组件,提供满足不同环境的执行脚本或者安装工具,提供命令行或者图形界面调试运行环境。
- f) 工具层具备可视化展示工具,提供后台系统展示相关的交易、统计、监控、日志等数据。

区块链中间件技术架构见图 1。区块链中间件接口描述参考见附录 A。区块链中间件应用方法见附录 B。





注 1：区块链中间件位于区块链和分布式记账技术架构中的服务接口层。  
注 2：区块链网络位于区块链和分布记账技术架构中的基础设施层与核心功能层。

图 1 区块链中间件技术架构

5.2 适配层

5.2.1 区块链接口协议适配

区块链接口协议适配,用于区块链中间件接入区块链网络,宜:

- a) 提供统一的适配层交互访问接口,供服务层调用;
- b) 提供统一的区块链网络交互访问接口,供适配层调用。

5.2.2 数据访问协议适配

数据访问协议适配,用于区块链中间件接入中间件数据库,宜:

- a) 支持主流的关系型数据库、非关系型数据库、内存数据库等,实现对不同类型中间件数据库的访问;
- b) 支持使用者自行搭建数据库或使用云服务数据库;

- c) 提供中间件数据库读写操作的功能,具备将数据解析为标准化结构数据的能力。

### 5.2.3 中间件数据库

中间件数据库用于保存网络信息、管理信息和监控信息等,宜具备以下要素:

- a) 网络信息包括业务系统、网络缓存、索引等数据;
- b) 管理信息包括节点信息、智能合约、权限、系统设置等数据;
- c) 监控信息包括系统资源、性能、统计分析、日志等数据。

## 5.3 服务层

### 5.3.1 总则

区块链中间件服务层核心功能,宜具备以下要素:

- a) 对适配层提供的数据进行解析、转换、加工,形成标准化结构数据;
- b) 对频繁请求数据的快速访问进行数据缓存;
- c) 定义中间件与多个接入的应用系统之间的关联关系;
- d) 在数据流转的各个环节保证数据的完整性与一致性;
- e) 提供同步或异步、实时或非实时等访问方式;
- f) 提供通用的且符合标准规范的功能接口。

### 5.3.2 管理组件

#### 5.3.2.1 概述

管理组件包括节点管理、合约管理、应用管理、权限管理、身份管理、全局设置等。

#### 5.3.2.2 节点管理

节点管理功能宜包括:

- a) 管理区块链节点,如节点加入、节点退出、节点删除等;
- b) 浏览区块链节点状态,如节点列表、节点所在 IP 地址等。

#### 5.3.2.3 合约管理

合约管理功能宜包括:

- a) 智能合约上传:开发者线下将应用系统的业务逻辑编写成智能合约,编译成功后上传;
- b) 智能合约验证:对合约进行静态验证等,以进行后续操作;
- c) 智能合约装载:部署智能合约,获得合约的区块链地址和合约的接口调用方式;
- d) 智能合约浏览:查询智能合约列表、当前的版本以及当前状态、区块链地址等;
- e) 智能合约冻结:冻结不再使用的智能合约;
- f) 智能合约升级:智能合约升级或回滚。

#### 5.3.2.4 应用管理

应用管理功能用于维护应用接入信息,宜包括:

- a) 管理应用,如创建应用、修改应用、移除应用等;
- b) 浏览应用,应用列表查询等。

#### 5.3.2.5 权限管理

权限管理功能宜包括:

- a) 访问控制权限管理：业务系统调用中间件接口提供权限控制管理能力，为应用系统分配 app\_id（应用唯一标识）、app\_key（公钥：相当于账号）、app\_secret（私钥：相当于密码）等；中间件接口的调用需进行签名与验签；
- b) 链用户管理：维护区块链链用户密钥信息；
- c) 登录用户管理：维护应用服务中间件管理系统登录账号信息；
- d) 登录角色管理：维护系统登录用户的角色信息，用于对管理工具的操作权限、接口调用权限的控制，可划分为如下用户角色：
  - 1) 普通操作角色：具有中间件管理平台的浏览查询权限，例如综合信息的查询；
  - 2) 开发角色：具有中间件接口的调用权限，例如智能合约的调用；
  - 3) 普通管理员角色：具有业务系统使用范围内的操作权限，例如节点管理、合约管理等；
  - 4) 超级管理员角色：拥有管理平台的所有操作权限，例如部署合约、冻结合约等。

5.3.2.6 身份管理

区块链网络采用基于数字证书的用户身份认证方式，身份管理功能宜包括：

- a) 数字证书导入，包括对应节点的链证书、机构证书、节点证书等；
- b) 查看数字证书详情，包括用户身份信息、用户公钥信息、CA 数字签名及有效期等；
- c) 下载数字证书。

5.3.2.7 全局设置



全局设置功能宜包括：

- a) 中间件接口调用频率设置；
- b) 用户数据上链（交易）总量限制设置；
- c) 上链数据检查规则设置；
- d) 异常告警类的配置。

5.3.3 信息查询组件

5.3.3.1 概述

业务数据经过中间件上链后保存在区块链上，业务应用系统可调用中间件信息查询组件获取业务信息与状态。中间件可提供同步机制，分析区块链上的数据，建立一套高效的索引（映射关系）。业务应用系统调用中间件的查询接口，中间件通过索引可检索所需的业务数据。

信息查询组件主要包含基本信息查询、交易信息查询、综合信息查询等功能。

5.3.3.2 基本信息查询

基本信息查询结果宜包括：

- a) 区块链的信息：当前区块高度、交易总量、区块数据等信息；
- b) 智能合约信息：智能合约的事件、合约地址、构造函数、执行函数等信息；
- c) 节点信息：节点列表与节点状态等信息。

5.3.3.3 交易信息查询

交易信息查询结果宜包括：

- a) 交易的哈希（hash）地址；
- b) 交易数据：上链业务数据；

- c) 交易时间;数据上链时间;
- d) 交易状态。

#### 5.3.3.4 综合信息查询

综合信息查询结果宜包括除基本信息和交易信息以外的其他业务信息。

### 5.3.4 监控服务组件

#### 5.3.4.1 概述

监控服务组件包括状态监控、交易审计、日志管理、异常告警等。

#### 5.3.4.2 状态监控

状态监控组件的监控内容宜包括:

- a) 区块链节点的加入、退出等状态;
- b) 智能合约的生命周期状态;
- c) 服务器资源状态。

#### 5.3.4.3 交易审计

交易审计组件用于对业务数据上链的过程信息进行跟踪审计,内容宜包括:

- a) 数据上链前检查;
- b) 数据上链时间;
- c) 数据上链总量;
- d) 数据上链吞吐量;
- e) 数据上链异常、失败、重试等信息。

#### 5.3.4.4 日志管理

日志管理组件用于问题追踪、预警与深入分析,支持对日志级别(包括警告、信息、错误等)进行灵活调整,内容宜包括:

- a) 系统运行信息;
- b) 管理操作信息;
- c) 数据处理信息;
- d) 中间件接口调用信息。

#### 5.3.4.5 异常告警

异常告警组件用于对状态监控、交易审计、日志管理中出现的异常信息进行告警,宜:

- a) 采用实时的方式(如邮件、短信、语音电话等)通知系统管理员,并对异常信息进行记录;
- b) 支持异常告警信息的分类、自定义通知方式等。

### 5.4 工具层

#### 5.4.1 可视化展示工具

区块链中间件宜提供可视化展示工具,内容宜包括:

- a) 统计数据:节点、区块、交易、合约等数据的多维度统计分析结果;
- b) 交易数据:交易详细信息的浏览查询结果;

- c) 监控数据：系统资源、性能、接口调用、异常信息的查询分析结果；
- d) 日志数据：系统运行、管理操作、数据处理、中间件接口调用等信息的查询分析结果；
- e) 访问记录：管理员操作使用的行为记录。

5.4.2 安装工具

安装工具宜提供快速部署安装方法。

5.4.3 配置工具

配置工具宜提供快速便捷接入区块链网络和访问中间件数据库的方法。

5.4.4 调试工具

调试工具宜提供区块链中间件的调试方法，快速定位问题。

6 非功能性指南

6.1 可靠性

区块链中间件符合可靠性要求，宜具备以下要素：

- a) 所使用的物理设备及环境有完善的监控体系，保证 7×24 h 稳定运行，系统具备高可用性，达到 GB/T 22239—2019 规定的第三级基本要求；
- b) 采取措施保障应用服务中间件的安全，预防非授权的访问或破坏，对于非授权的访问或破坏具有防护措施和应急预案；
- c) 提供集群特性，避免单点失效；
- d) 具备冗余备份和存储扩展的能力，当中间件出现故障时，保证区块链与应用系统数据的完整性。



6.2 可维护性

区块链中间件符合可维护性要求，宜具备以下要素：

- a) 提供便捷的安装部署方式；
- b) 提供应用接入定制开发接口，以适应不断变化的业务新需求；
- c) 提供必要的日志记录；
- d) 提供用于故障排查、系统监控及管理的工具。

6.3 兼容性

区块链中间件符合兼容性要求，宜具备以下要素：

- a) 在不同区块链网络上提供的应用开发接口保持一致性；
- b) 兼容多种主流的服务器操作系统；
- c) 兼容旧版本。

6.4 性能指南

区块链中间件符合相关效率指标，宜具备以下要素：

- a) TPS：区块链中间件每秒可处理的事务数；
- b) 延迟：业务应用提交事务到数据上链的时间；
- c) QPS：中间件信息查询接口的每秒响应请求数；
- d) 容量：中间件数据库存储各类数据的承载能力。



附录 A  
(资料性)  
区块链中间件接口描述参考

A.1 数据上链交易接口

数据上链交易接口用于业务应用系统的数据信息上链，接口描述见表 A.1。

表 A.1 数据上链交易接口描述

类别	参数名称	描述
接口 URL 地址	—	http://ip:port/middleware/transaction/write
调用方法	—	POST
输入参数	数据签名相关参数	如 app_id,app_key,app_sign 签名串等
	业务 id	应用系统业务的唯一标识符
	合约地址	智能合约装载成功后得到的地址
	调用方法名	类型为 string
	方法参数	类型为 json 格式的字符串
返回参数	Code	状态码
	Message	提示信息
	Data	返回的数据,包含交易 id 号等

A.2 交易查询接口

交易查询接口用于业务应用系统查询交易信息，接口描述见表 A.2。

表 A.2 交易查询接口描述

类别	参数名称	描述
接口 URL 地址	—	http://ip:port/middleware/transaction/get
调用方法	—	POST
输入参数	数据签名相关参数	如 app_id,app_key,app_sign 签名串等
	业务 id	应用系统业务的唯一标识符
返回参数	Code	状态码
	Message	提示信息
	Data	返回的数据,包含业务 id、交易 id、合约地址、方法名、方法参数、用户 id、当前状态、交易 hash、交易返回原文信息、交易回执状态、提交时间、上链时间等

附 录 B  
(资料性)  
区块链中间件应用方法

B.1 中间件部署方式

区块链中间件宜支持多种方式部署,包括物理机部署、云部署和容器化部署等。

B.2 业务应用系统接入方式

业务应用系统接入区块链中间件的方式包括:

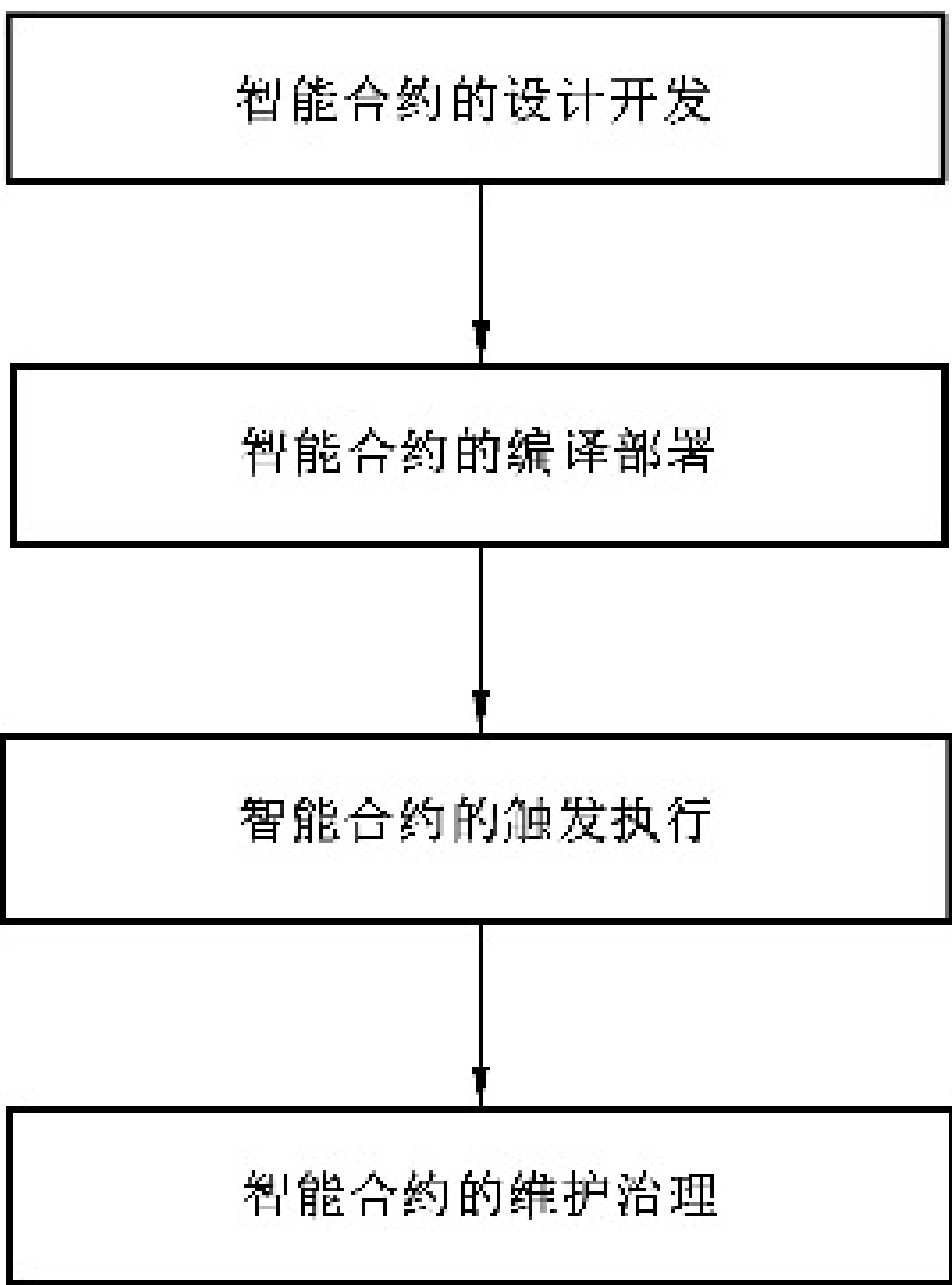
- a) 当完全使用中间件系统时,可基于中间件接口进行二次开发,适用于不具备区块链原生接口开发能力的开发人员;
- b) 当部分使用中间件组件时,可使用中间件的节点管理、监控服务组件用于管理监控,业务应用系统调用区块链原生接口进行开发,适用于具备区块链原生接口开发能力的开发人员;
- c) 当选择性使用中间件组件时,可与区块链原生接口搭配使用,适用于掌握区块链底层开发技术的开发人员。

B.3 智能合约管理

区块链中间件安装部署完毕后,可通过管理组件配置完成区块链网络的接入,由业务应用系统进行接口调用。

业务应用系统在接入中间件前,开发人员应根据接入的区块链网络,自行开发包含区块链应用业务逻辑的智能合约。智能合约管理是中间件的核心组件。在智能合约编译成功后,可以通过中间件管理组件完成上传,安装与部署。业务应用系统可通过中间件接口执行交易事务处理、数据上链和数据查询等操作。智能合约可通过配置工具进行管理,通过调试工具解决实际部署中出现的问题。

智能合约的接入流程包括智能合约的设计开发、智能合约的编译部署、智能合约的触发执行、智能合约的维护治理,接入流程见图 B.1。



- 注 1：智能合约的设计开发：基于业务需求完成智能合约的功能设计，开发人员根据接入的区块链网络类型编写调试智能合约代码。
- 注 2：智能合约的编译部署：将智能合约代码转换成运行环境可执行格式，通过中间件配置工具上传，由中间件部署到智能合约运行时环境中。
- 注 3：智能合约的触发执行：中间件管理组件获取合约的区块链地址和合约接口可调用的方法与参数；满足条件的事件通过中间件推送到区块链网络执行，将事件和执行结果计入区块链。
- 注 4：智能合约的维护治理：智能合约安装部署过程中，若存在失败的情况，节点管理组件中展示失败的详情，管理用户根据失败详情修改合约后再次上传；智能合约成功部署上线后，因修正错误、提升性能等需求，需进行智能合约的升级、冻结、废止等操作。

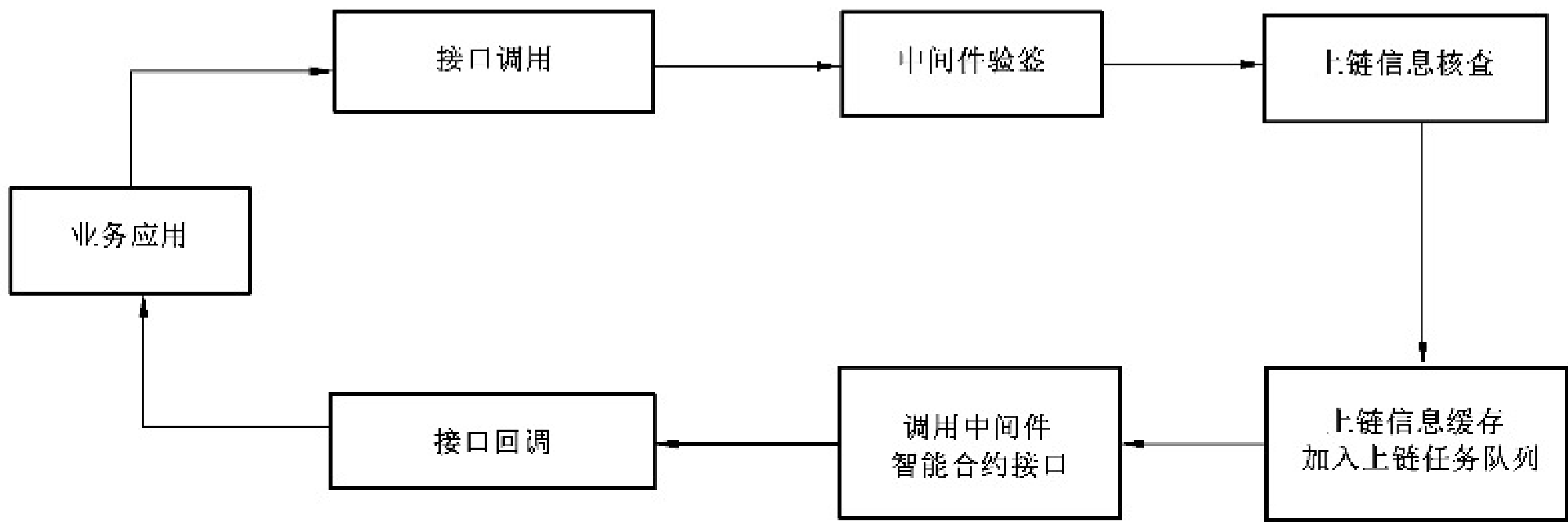
图 B.1 智能合约接入流程

B.4 数据上链流程

数据上链前，宜通过节点管理组件完成智能合约的部署，并给业务系统分配账号以及对应账号的访问权限。数据上链流程包括应用端接口调用、中间件验签、上链信息核查、上链信息缓存、加入上链任务队列、调用中间件智能合约接口、接口回调，数据上链流程见图 B.2。







- 注 1：业务应用接口调用：将业务数据转换成中间件数据格式，调用中间件上链交易接口。
- 注 2：中间件验签：对中间件 API 进行签名验签。
- 注 3：上链信息核查：检查上链信息是否符合要求，检查上链交易是否达到了阈值。
- 注 4：上链信息缓存：上链信息保存在中间件数据库中。
- 注 5：加入上链任务队列：将上链请求转化为任务队列。
- 注 6：调用中间件智能合约接口：通过执行智能合约方法，将数据写入区块链中。
- 注 7：接口回调：中间件返回交易状态信息。

图 B.2 数据上链流程

参 考 文 献

- [1] GB/T 30275—2013 信息安全技术 鉴别与授权 认证中间件框架与接口规范
  - [2] GB/T 36960—2018 信息安全技术 鉴别与授权 访问控制中间件框架与接口
- 



