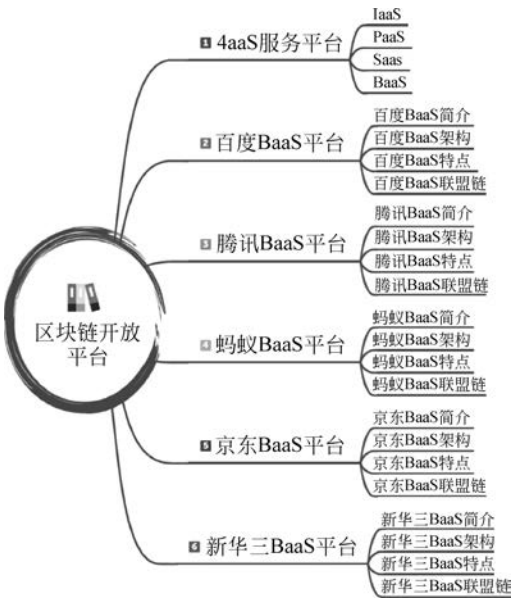
第5章

区块链开放平台

本章思维导图



第4章概要介绍了各大开源软件的特性和编译、安装，起到了抛砖引玉的作用。对于每个开源软件，要想使用它进行二次开发，需要进行深入研究。可以学习这些开源软件的设计思想，读者只要有一定的技术基础，就可以基于这些开源软件搭建自己的区块链，不过这些开源软件更新太快，在搭建的过程中可能会遇到一些问题。

基于这些开源软件，国内的各大云服务厂商(如BATJ)都推出了各自的BaaS平台，用户可以很轻松地在这些平台上创建自己的联盟链。

目前平台架构有IaaS、PaaS、BaaS、SaaS 4种，简称4aaS服务平台，这4种平台有各自的定位。本章先阐述这4种服务平台的区别，然后逐一介绍市面上主流的BaaS平台。

5.1 4aaS服务平台

如图5-1所示，IaaS、PaaS、BaaS和SaaS就是云服务提供的4种层次，最基础的是IaaS，中间的为PaaS和BaaS，最后直观呈现出来的是SaaS。

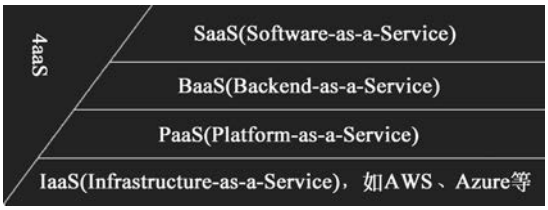


图 5-1　云服务类型

5.1.1　IaaS

IaaS 的全称是 Infrastructure-as-a-Service(基础设施即服务)，即云计算交付模式，提供给客户的服务是对所有计算基础设施的利用，包括处理 CPU、内存、存储、网络和其他基本的计算资源，用户能够部署和运行任意软件，包括操作系统和应用程序。

在这种服务模型中，用户不用自己构建硬件设施，而是通过租用的方式，利用 Internet 从 IaaS 服务商获得计算机基础设施服务，包括服务器、存储和网络等服务。IaaS 服务商根据用户对资源的实际使用量或占有量进行计费。在使用模式上，IaaS 与传统的主机托管有相似之处，但是在服务的灵活性、扩展性和成本等方面具有很强的优势。

主流的 IaaS 服务商有 Amazon、Microsoft Azure、VMware、阿里云等。

5.1.2　PaaS

PaaS 的全称是 Platform-as-a-Service(平台即服务)，有时也叫作中间件，是云计算的重要组成部分，提供运算平台与解决方案服务，为某些软件提供云组件，这些组件主要用于应用程序。在云计算的典型层级中，PaaS 层介于 Saas 与 IaaS 之间。PaaS 服务商提供各种开发和分发应用的解决方案，如虚拟服务器和操作系统、应用开发、存储、安全等工具。

PaaS 提供了一个基于 Web 的软件创建平台，使开发人员可以自由地专注于创建软件，同时不必担心操作系统、软件更新、存储或基础架构。

PaaS 抽象了硬件和操作系统细节，可以无缝地扩展(scaling)。开发者只需要关注自己的业务逻辑，不需要关注底层。

主流的 PaaS 服务商有 Google App Engine、OpenShift、CloudFoundry 等。

5.1.3　SaaS

Saas 的全称是 Software-as-a-Service(软件即服务)。软件的开发、管理、部署都交给 SaaS 服务商，客户不需要关心技术问题，可以拿来即用。SaaS 代表了云市场中企业最常用的选项，利用互联网向其用户提供应用程序，而这些应用程序由第三方供应商管理。大多数 SaaS 应用程序可以直接通过 Web 浏览器运行，不需要在客户端进行任何下载或安装。

主流的 SaaS 服务商有 Salesforce、Zoom、腾讯会议等。

5.1.4　BaaS

Baas 的全称是 Backend-as-a-Service(后端即服务)。BaaS 公司为移动应用开发者提供整合云后端的边界服务，为应用开发提供后台的云服务，其架构如图 5-2 所示。

BaaS 平台使用示例

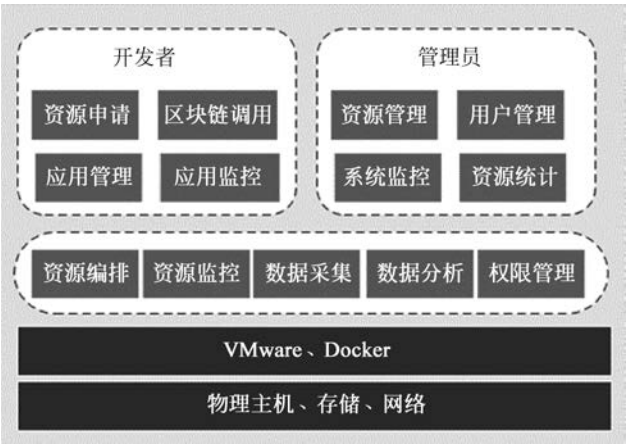


图 5-2 BaaS 平台基础架构

BaaS 分为公有云和私有云。公有云面向开发者提供运营服务；企业私有云是企业构建移动信息化应用的基础平台，大量的移动应用基于该平台开发和管理，能有效地降低企业的移动信息化成本。

国内的主流区块链 BaaS 平台有百度、腾讯、蚂蚁、京东、新华三等。

5.2 百度 BaaS 平台

百度 BaaS 平台的网址为 https://console.bce.baidu.com/bbe/#/bbe/block/list。

5.2.1 简介

百度 BaaS 平台，也称为百度区块链引擎（Baidu Blockchain Engine，BBE），是为用户提供全面的云端区块链服务平台，能快速地为企业和开发者在公有云、私有云中搭建区块链网络，支持 Fabric、Quorum 等多种技术框架的联盟链以及多种框架的私有链，支持多链架构、跨链数据同步、可信计算、链上链下安全、多层级激励体系等。适配企业对于多账本、隐私交易等多场景的需求；同时兼容外部联盟链，支持接入行业联盟链（十二行联盟、中国贸易金融跨行交易联盟）。

百度 BaaS 平台基于百度云容器引擎 CCE，用户仅需要根据企业对于区块链网络的需求进行简单的参数配置，即可搭建出符合业务要求的区块链网络。解决了区块链网络到业务系统构建的“最后一公里”，让企业开发者快速完成基于区块链网络开发和搭建可信的去中心化业务系统，如图 5-3 所示。

（1）合约网关 RESTful API。

开发以太坊 Dapp，与智能合约交互时通常使用 Web3，这种方式需要开发者管理 Nonce、构建交易、签名交易、解析合约返回数据等，并且在调用过程中容易出现各种错误，没有很好的提示和处理机制，对开发人员来说并不友好。基于此，百度公司开发的以太坊合约网关旨在为用户提供企业级的合约管理服务，使用传统的 RESTful API 设计让应用开发人员聚焦于自身的业务逻辑和用户体验，将复杂的合约事务提交、Nonce 管理等交由合约网

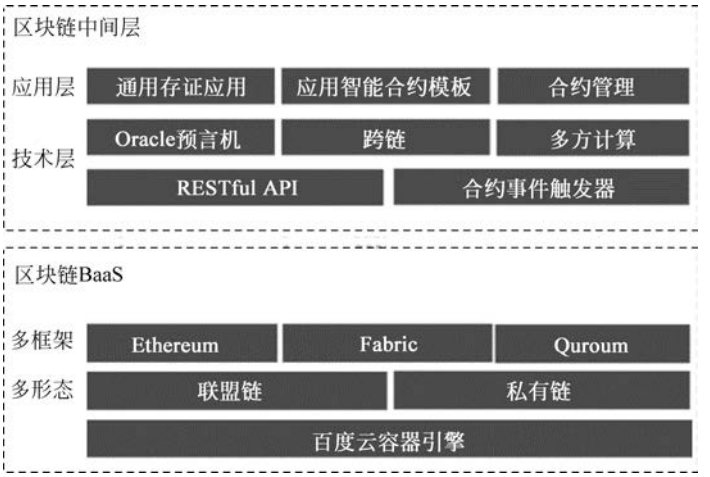


图 5-3　百度 BaaS 平台与区块链中间层

关来处理。

(2) Oracle 预言机。

由于区块链是确定性的环境,它不允许不确定的事情或因素,智能合约不管何时何地运行都必须是一致的结果,所以虚拟机(EVM)不能让智能合约有网络调用,不然结果就是不确定的。而这个特性大大限制了 DApp 的发展,因为很多 DApp 都需要与链下数据进行交互。所以区块链只能由特定的服务把外部数据传递给区块链上的智能合约,这个特定的服务就被称为 Oracle 预言机。BBE 提供封装好的、基于 SGX 和 MesaTEE 的 Oracle 可信预言机,可以让用户快捷地实现链上、链下数据打通。

(3) 通用存证 API。

无须浪费精力于研究如何开发智能合约,BBE 提供通用存证 API,封装区块链与智能合约间的复杂交互,企业开发者使用传统的 API 方式即可将业务系统与区块链底层网络打通。同时,支持用户自定义存证内容的关键字段,满足用户多样的存证诉求。在此之上,提供大文件哈希存证、音频视频指纹提取存证、基于 IPFS 的分布式存储等技术解决方案,适用于多种存证场景。

5.2.2　架构

百度 BaaS 平台的技术框架分为两大部分:百度区块链商业化技术栈和商业化技术能力。技术栈核心主要包括三大部分:区块链 PaaS、区块链 Framework、区块链中间层。百度区块链平台是由这三层技术栈合力驱动的,形成一个完备的商业化技术方案,其框架如图 5-4 所示。

1. 区块链 PaaS

区块链 PaaS 是为了解决商业化环境的差异性问题。PaaS 层能够对上层的区块链 Framework 屏蔽资源环境因素,引入了基于 Kubernetes 和 Docker 的容器集群引擎、镜像仓库和函数计算等能力,实现了计算和存储资源的统一化抽象和高效利用,还提供了镜像级的版本管理和函数式的合约编程框架。

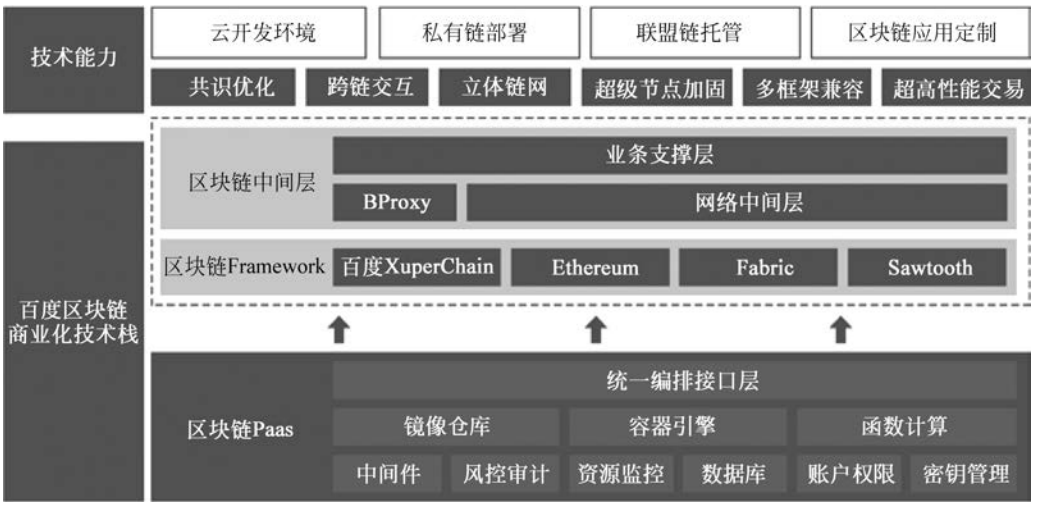


图 5-4　百度区块链框架

区块链 PaaS 在顶层封装了统一的编排 API 层。编排 API 整体面向资源，包括函数计算任务资源、镜像资源、实例容器资源和其他基础资源，统一资源调度动作描述和描述结构体，可以简化上层 Framework 调用不同服务的复杂性。

2. 区块链 Framework

区块链 Framework 层主要解决以下三个问题。

（1）多种区块链网络的兼容部署。

在节点部署、合约部署、DApp 部署全流程中支持 XuperChain 的一键部署，同时也支持以太坊、Fabric 等其他开源框架。

（2）多种区块链网络的托管和监控方案。

区块链 PaaS 层提供了资源 failover 策略，保证网络节点故障可自动恢复；还提供了不同区块链框架的兼容性监控方案，指标包括链上区块数、出块速度、单位块验证速度、每秒交易数（TPS）、每区块交易数、子链数、跨链交互次数、机构数等。

（3）多种区块链网络的交互逻辑抽象。

部署区块链网络的流程可以归纳为“配参＋部署”的交互逻辑，其中配参包括的参数项有框架类型、联盟参与方信息、网络规模、账号、合约和 DApp 等信息。

平台将使用 Framework 预设逻辑调用区块链 PaaS 接口进行一键式部署。

3. 区块链 BProxy

区块链 BProxy 是一个代理模块，解决了多种区块链方案私有化场景的适配问题，实现了多方的身份互信管理，同时也在跨网环境中解决了数据上链的问题。

4. 区块链网络中间层

不同的区块链框架偏向不同的交易类型，区块链网络中间层完成了跨链数据的结合读写，通过与不同类型的区块链网络交互，完成多类型数据的事务性同步，直接与 DApp 进行数据交互。

5. 区块链业务支撑层

区块链业务支撑层主要为了将不同业务应用与底层区块链方案进行实际解耦，支持数

据和签名的差异化存储上链，提供场景化的身份定义，同时平台在业务支撑层增加了通用的合约基础库和合约模板。

5.2.3　特点

1. 可信计算环境

BBE 基于以下多个维度的可信计算环境支持，实现全方位区块链网络安全保护，全时段维护业务链上的应用信息、数据、执行逻辑的安全可信。

（1）多级加密技术。

支持数据上链、数据传输、合约调用等多流程多种加密算法逐级加密及验证，如图 5-5 所示。

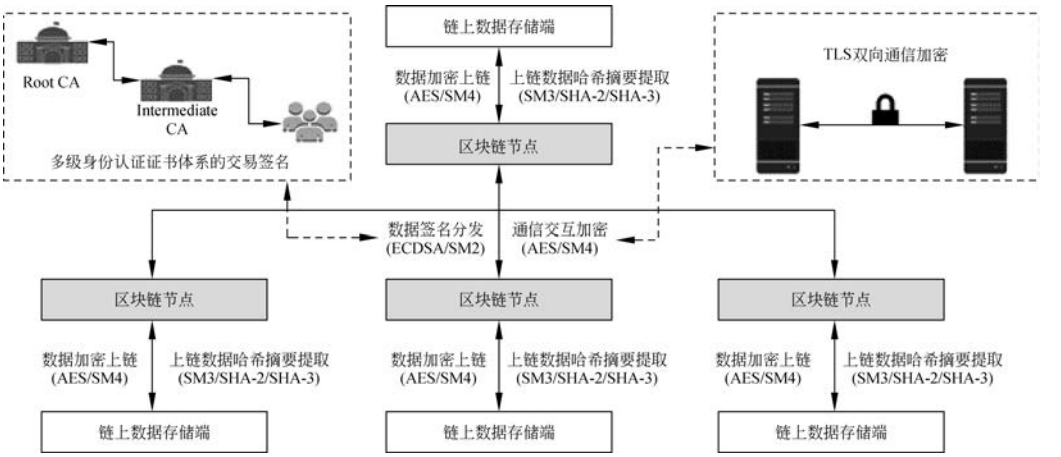


图 5-5　多级加密机制

（2）国际/国密标准的加密算法支持。

- 非对称加密算法：SM2、ECC；
- 哈希算法：SM3、SHA-2、SHA-3；
- 对称加密算法：SM4、AES、DES。

（3）跨链网安全代理：多架构、多类别跨链数据交互及合约调用通过安全代理模块支持跨链数据安全的加密及安全准入、审计控制。

（4）基于可信硬件的自研合约安全执行环境。

2. 高性能高吞吐

实现基于公有链、私有链、联盟链的多链架构，支持区块链网络及链上应用的规模性增长。用户可根据业务场景需求选择区块链架构，进行链网参数优化及共识机制切换，突破性能与吞吐的极限。

（1）适配不同业务场景的多种共识机制：针对 BBE 跨链架构及具体业务场景，提供针对公有链、私有链及联盟链的多种共识机制支持。

- 公有链场景下，百度超级链实现了基于时序的 TDPOS 共识算法，支持 20 000＋TPS；
- 联盟链场景下实现了 Paxos/Raft/PBFT 等多种共识机制，最大可支持 10 000＋TPS。

（2）基于以太坊的私有链场景可选 POW、POA、DPOS 等多种共识机制。

（3）支持多链架构水平动态扩容和缩容。

（4）基于轻量级内存缓存的架构优化。

3. 可扩展的存储

区块链通过节点间存储的高冗余来保障链上数据的高可用和安全性。这也就意味着相比于中心化的存储系统，区块链网络保存的数据副本基本上随节点规模线性增长。反之，由于世界状态的不可破坏性，区块链中每个节点都会尽量多地保存原始的全局数据，包括状态数据、交易数据、交易凭证甚至事件数据都会持久化到节点存储中。在实际生产环境中，区块链节点需要的存储空间大小会随着交易数量的增加而持续增长。

百度智能云提供无限量的存储空间，并达到数据可用性和数据安全性的业界标准。同时，百度智能云结合云存储，深度定制区块链节点存储机制，实现区块链专有的存储技术。

4. 数据热度自适应存储

实现冷热数据自适应调度，支持分布式文件系统，存储容量理论上可以扩展到 PB 级。状态数据一般位于块头，是链上各区块的索引数据。系统通过标记块头状态索引计数，将已被覆盖的状态索引踢出块头，从而保证状态数据量与高频覆写交易量解耦。将低频变更的状态数据分代迁移到成本更低的 SATA 介质或者云存储，高频变更的状态数据存放在内存和 SSD 介质的数据库中。同样，从数据库中读取状态节点时，本着最小 I/O 开销的原则，仅读取那些需要用到的节点数据。根据读取频率，状态节点的索引路径也会根据热度进行打分，状态树被划分为冷热区，冷区状态节点会迁移到成本更低的存储介质中。

多用户访问控制主要用于帮助用户管理云账户下资源的访问权限，适用于企业内的不同角色，可以给不同的工作人员赋予使用产品的不同权限。

5.2.4 创建联盟链

用户需要先创建组织，再以组织的身份创建或加入联盟。一个组织可以加入多个联盟，但对于某个联盟只允许用户的一个组织加入。

联盟是由多个组织组成，联盟创建者即为盟主，加入联盟者为成员组织。

（1）创建组织 1，使用组织 1 创建联盟；

（2）邀请用户 2；

（3）用户 2 接受邀请，创建组织 2，并发起加入联盟申请；

（4）待审批通过后用户 2 使用组织 2 加入联盟；

（5）部署智能合约；

（6）部署 DApp；

（7）发起隐私交易。

对于区块链的便签板应用，只有参与隐私交易的成员才能添加、更新和查看便签。

关于用户授权，在“用户管理”→“子用户管理列表”中对应子用户的“操作”列选择“添加权限”，可以为用户选择系统权限或通过自定义策略进行授权。

说明：如果要在不修改已有策略规则的情况下修改某子用户的权限，只能通过删除已有的策略并添加新的策略来实现，不能取消勾选已经添加的策略权限。

5.3 腾讯 BaaS 平台

腾讯 BaaS 平台的网址为 https://baas.qq.com/doc/dev.shtml。

5.3.1 简介

腾讯区块链以自主可控的区块链基础设施，基于场景构建安全高效的解决方案。为整体应用框架秉持区块链的分布式、弱中心、自组织精神，尽可能地弱化各个节点在业务开展过程中对中心化设施的依赖，并且能解决应用从前到后全生命周期的问题。

腾讯区块链主要包括 BaaS 和 TrustSQL 两部分。BaaS 主要提供商户注册、链、节点信息查询以及一些链的操作，商户注册成功之后，通过 BaaS 可以获取机构 ID、链信息等，这些信息是后续接口服务的必要信息。TrustSQL 是腾讯区块链的底层服务，主要提供交易的插入、交易的查询等操作，用户可以直接针对这一层进行开发。

为了更好地让用户快速接入腾讯区块链，对 TrustSQL 提供了上层接口封装，主要有两种，即数字资产服务和共享信息服务，这两种服务提供 rest 风格的接口，可以很方便地接入。数字资产服务、共享信息服务及 TrustSQL 服务都是去中心化的，以镜像的形式部署到节点上，并有操作权限的控制，用户可以根据自己的需要关闭和打开接口。

为了减少用户接入的成本，针对市场上主流的开发语言，提供了 Java、C++的 SDK，主要用于签名、验签、生成公私钥、根据公私钥生成地址，以及生成一些 demo。

5.3.2 架构

腾讯区块链从技术实现上可以把区块链整体应用分为四层：区块链基础服务层、行业应用服务层、业务逻辑表现层、联盟治理层。整体应用框架如图 5-6 所示。

图 5-6 腾讯区块链架构

- 区块链基础服务层、行业应用服务层、业务逻辑表现层属于节点软件范畴，应部署于各自的节点上，属于联盟成员的自有设施。
- 联盟治理层属于联盟的公共设施，应部署于联盟委员会性质的中立节点上，目前可由区块链技术服务商来进行运营，便于维护升级。

以上两类分层属于不同维度，因此联盟链的管理者与节点的所有者权限各不相同。

BaaS 开放平台为腾讯区块链提供的企业级区块链应用开放平台，客户可使用测试链进行服务测试或搭建自己专属的联盟链。根据 1.2.1 节中的总体设计，BaaS 开放平台整体架构设计分为两部分：链管理平台和节点管理平台。

链管理平台是中心化管理平台，负责建链及链、节点、成员的管理，不涉及业务逻辑与读写数据。主要用于联盟链的搭建以及节点、成员的增删等。

节点管理平台是去中心化管理平台，部署于节点本地，提供节点本地工具，帮助用户管理数据和业务逻辑，具备用户公钥管理及区块链浏览器等功能。

两个平台的区别与联系如图 5-7 所示。

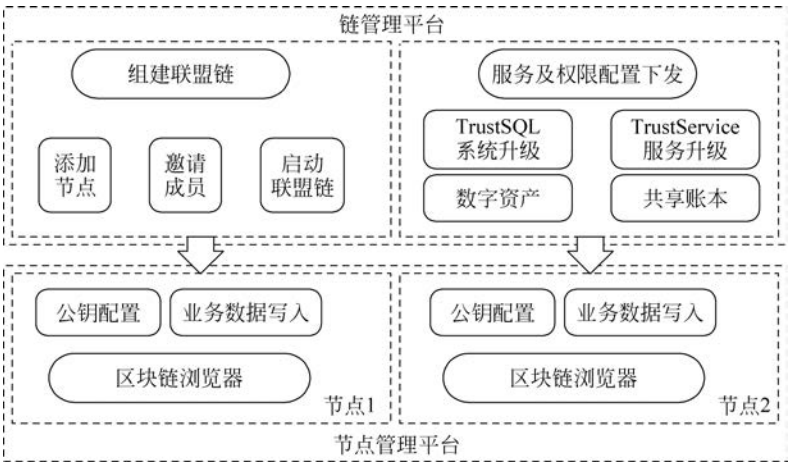


图 5-7　链管理平台与节点管理平台

（1）链管理平台进行联盟链维度的管理，偏重于管理功能，提供 BaaS 级功能 API 以供调用（区块链浏览器、TPKI 接口文档），不涉及节点上的业务数据。链的所有者与参与者均可以注册登录 BaaS 平台进行注册登录，查看及管理自己所创建或参与的联盟链。

（2）节点管理平台进行节点维度的管理，偏重于业务功能，提供部署于各个节点上的节点级功能 API（数字资产、共享账本、区块链浏览器）以供调用。节点的所有者可以登录自己的节点管理平台，查看及管理自己所拥有的节点与链上数据。

（3）使用两个平台 API 的用户均需要上传对应的公钥，用来完成对应 API 接口的通信校验（上传公钥）。

5.3.3　特点

TrustSQL 的接入方式和 MySQL 类似，如表 5-1 所示。

表 5-1　MySQL 和 TrustSQL 的比较

项目	MySQL	TrustSQL
协议	MySQL 协议	兼容 MySQL 协议
支持的操作	CURD	仅支持 Insert 和 Select
插入操作	随意插入	所有入链的数据需要使用私链进行签名
查询操作	随意查询	兼容 MySQL 查询

TrustSQL 统一采用 ECDSA 进行数字签名，曲线选择与比特币相同，即 secp256k1。

公钥和私钥：采用 secp256k1 椭圆曲线生成一对公钥和私钥，或者通过私钥可以算出公钥。在 TrustSQL 中公钥和私钥的编码格式为 Base64。

地址：通过私钥可以算出公钥，通过公钥可以算出地址。在 TrustSQL 中地址的编码格式为 Base58。

智能合约：腾讯智能合约的特殊之处如表 5-2 所示。

表 5-2　腾讯智能合约的特殊之处

	内置合约	常见区块链锁
加载方式	以 so、JAR 包形式嵌入共识逻辑层或使用合约语言(目前支持 JavaScript)，由参与的多方链达成线下共识之后，动态加载到区块链上来	合约在独立环境(Docker 中执行 JVM、Go)，由参与的任意节点编写
特点	1. 允许有限的合约编写； 2. 与共识逻辑一体，无独立执行环境中的安全隐患； 3. 执行效率更高	1. 灵活性强，合约数量几乎无限制； 2. 独立执行环境安全性挑战大； 3. 逻辑复杂，执行效率低
适合场景	更适合联盟链，稳定且有重点地解决有限个核心诉求	更适用于公有链，自由创新合约逻辑

5.3.4　创建联盟链

开发者可在“链管理”页面新建专属联盟链，单击“新建联盟链”按钮，则进入建链流程。建链流程共分为四个步骤，依次为新建联盟链、添加节点、邀请成员和启动联盟链。建链流程如图 5-8 所示。

图 5-8　建链操作流程

说明：客户新建联盟链时，如中途中断、未完成整体流程，则在“链管理”页面单击“查看”按钮，可以继续完成建链。

1. 新建联盟链

新建联盟链主要是为该联盟链命名，即完成相关描述。此处已经产生该联盟链的链 ID(chain_id)，即使未完成建链的后续操作，该链也已经存在，可后面继续完成。

2. 添加节点

联盟链由节点组成，且一条联盟链至少需要 4 个节点共同参与才能运行。此处主要在新建联盟链的流程中为该联盟链添加节点，即此处添加的节点都会添加到该联盟链上。每个联盟链的参与方都可以提供一个或多个节点参与到联盟链中。有三种方式可添加节点，分别是：购买节点，添加已关联节点，关联已有腾讯云机器。

3. 邀请成员

邀请其他机构进入联盟链。根据被邀请方是否需要自带节点进入联盟链，可分为两类：分配节点和自带节点。

分配节点：即联盟的创建方提供多个节点，并将自己的节点分配给其他联盟链的参与方，该节点的使用权限则归属被分配方。

自带节点：即联盟链创建方邀请其他机构参与联盟链的共同建设，其他机构需要自带节点加入联盟链。

4. 启动联盟链

启动一条联盟链至少需要 4 个节点。当满足该条件时，即可启动、运行一条联盟链。

5.4 蚂蚁 BaaS 平台

蚂蚁 BaaS 平台的网址为 https://antchain.antgroup.com/products/baas。

5.4.1 简介

蚂蚁 BaaS 平台是蚂蚁金服自主研发的具备高性能、强隐私保护的金融级区块链技术平台。该平台提供一站式服务，有效解决金融、零售、生活等多场景下的区块链应用问题。

该平台以联盟链为目标，提供简单易用、一键部署、快速验证、灵活可定制的区块链服务，加速区块链业务应用的开发、测试、上线，助力各行业区块链的商业应用场景落地。提供高性能、稳定可靠、隐私安全、支持多种类型数据的区块链存证能力。

该平台基于蚂蚁区块链提供基础技术能力，并输出定制化的区块链整体解决方案，应用于诸如数据存证与溯源、多方参与的业务协同、资产登记流转等场景。

5.4.2 架构

蚂蚁区块链通过引入 P2P 网络、共识算法、虚拟机、智能合约、密码学、数据存储等技术特性，构建一个稳定、高效、安全的图灵完备的智能合约执行环境，提供账户的基本操作以及面向智能合约的功能调用。基于蚂蚁区块链提供的能力，应用开发者能够完成基本的账户创建、合约调用、结果查询、事件监听等。其架构如图 5-9 所示。

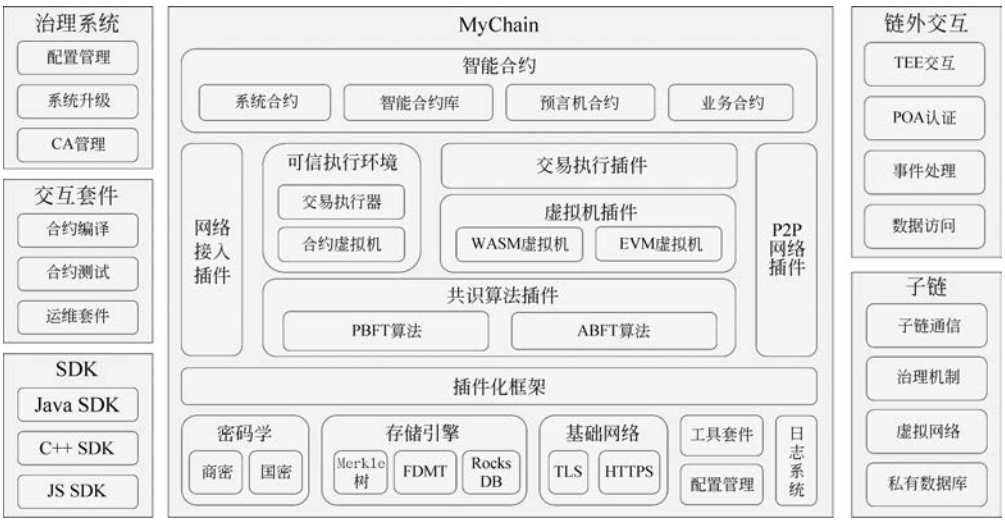


图 5-9 蚂蚁区块链的架构

其核心逻辑如图 5-10 所示。

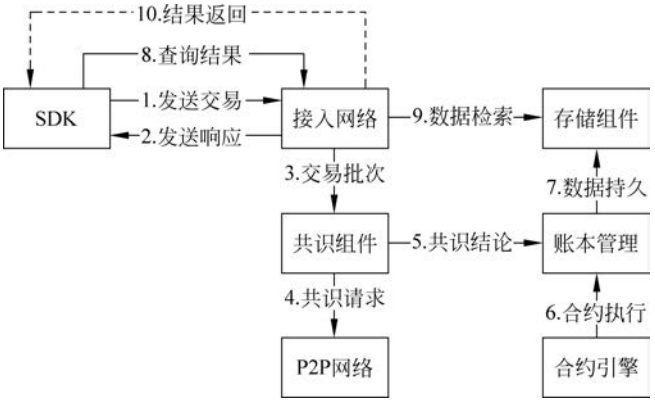


图 5-10　蚂蚁区块链的核心逻辑

基于蚂蚁区块链开发应用时，可以有以下 3 种选择。

选项 1：通过 SDK 在命令行与蚂蚁区块链交互。

选项 2：通过 Web 应用(Client)集成 SDK 直接与蚂蚁区块链交互。该方式让客户端直接访问区块链平台，去掉了中间的后端服务，更加透明，比较适合轻量级的合约调用、查询等操作。

选项 3：与传统 Web 应用开发相似，访问后端服务(Service)，后端服务集成 SDK 后与蚂蚁区块链交互。该方式适合与传统的业务系统相结合，在后端服务层实现比较重要的业务逻辑和计算任务。

在实际操作中，选项 2 和选项 3 比较常用，可以根据具体应用场景进行选择。

5.4.3　特点

1. 账户模型与状态转换

蚂蚁区块链采用的新型账户模型设计能够支持多重签名机制与私钥恢复机制，从而解决了账户控制权重问题与单一私钥丢失导致账户不可用的问题。

出于安全性考虑，蚂蚁区块链基于密码学与链式结构，通过签名机制实现交易数据的不可篡改性和不可伪造性。

2. 智能合约

智能合约实质上是一套以数字形式定义的承诺(Promises)，包括合约参与方可以在上面执行这些承诺的协议。蚂蚁区块链基于此定义设计了自己的智能合约平台，支持智能合约的拓展能力，能够基于智能合约编写图灵完备的业务逻辑来实现丰富的业务场景。

(1) 合约生命周期。

蚂蚁区块链中，一份智能合约的典型的生命周期覆盖合约编写、合约编译、合约部署、合约调用、合约升级、合约冻结 6 个环节。

(2) 合约类型。

蚂蚁区块链提供图灵完备的智能合约能力，目前提供对 EVM、Native、MYVM、Precompiled 这几种合约类型的支持。其中，MYVM 合约类型由蚂蚁自研的 MYVM 虚拟

机类型支持，以 LLVM(Low Level Virtual Machine)编译模型支持多种合约编程语言(如 Solidity 和 C++)，支持更优秀的性能以及更出色的开发者友好特性。

(3) 合约扩展。

蚂蚁区块链智能合约提供了多种形式的合约扩展能力，包括隐私保护、RSA 验签、Base64 编解码、上下文获取、JSON & XML 解析等。

3. 存储设计

蚂蚁区块链具备以下存储能力。

(1) 数据存储。

数据存储分为本地文件系统的 KV 数据库存储和上层的抽象世界状态数据存储。蚂蚁区块链智能合约平台的对象存储利用特定的树状数据结构存储数据来达到全局状态快速计算摘要。

(2) 世界状态存储。

蚂蚁区块链中，合约对象分为成员变量、成员函数。其中，成员变量存储在合约状态(Storage)中，成员函数存储在合约代码(Code)中。合约代码与合约状态数据分离，为合约状态和世界状态提供了唯一稳态哈希值的计算，同时支持树上节点快速索引和更新。

(3) 历史数据。

蚂蚁区块链中，不同的区块拥有不同的全局状态根哈希。根据不同区块和不同的全局状态根哈希，可以构造出不同的全局状态历史树，进而查询不同历史状态下的数据。

4. 共识协议

在蚂蚁区块链中，共识协议被定义成使分布式系统中的节点快速、有效地达成数据的一致性，即确保所有诚实节点以完全相同的顺序执行共识结论中的交易，达成数据一致性，同时正确的客户端发送的有效交易请求最终会被处理和应答。

蚂蚁区块链平台的共识组件通过提供不同的共识插件来实现共识协议。目前，蚂蚁区块链系统中已实现的共识算法包括 PBFT 和 HoneyBadgerBFT。

PBFT 共识协议支持系统中不超过 1/3 的节点容错性。通过 PrePrepare、Prepare、Commit 三阶段提交协议来实现网络共识节点之间的交易数据的一致性。蚂蚁区块链提供的 PBFT 共识插件具有快速终止、恢复可靠、状态同步等特性。

HoneyBadgerBFT 是一个满足拜占庭要求的异步共识协议，具备无主节点、异步交互、支持较大节点规模、拜占庭容错等优势，但实现的复杂程度较高。具体而言，蚂蚁区块链的 HoneyBadgerBFT 共识插件可以有效地降低网络带宽负载，以及避免选择性共识问题。

5. 虚拟机

虚拟机的职责是在特定的执行环境下通过一组指定的字节码指令来指定蚂蚁区块链状态机抽象模型的全局状态的更改方式。

除蚂蚁金服自主研发的类 EVM 虚拟机插件，蚂蚁区块链还提供 MYVM、Native 虚拟机插件。EVM 虚拟机插件支持流行的 Solidity 合约语言，MYVM 虚拟机插件以 LLVM 编译模型支持多种合约编程语言。

6. 安全机制与隐私保护

蚂蚁区块链的安全机制主要分为网络安全、数据安全、存储安全三个维度。

网络安全：客户端和节点通过 CA 中心获取 TLS 证书，客户端与节点之间、节点与节

点之间进行 TLS 双向认证，且通信流量经 TLS 加密，可抵御中间人攻击。除了基本的证书验证外，节点与节点之间还增加了握手逻辑，通过在握手过程中添加验证对方节点私钥签名的方式来确保节点间通信的可靠性。

数据安全：交易使用用户私钥签名，保证交易内容无法篡改。

存储安全：数据多节点存储，单节点数据丢失不影响整个网络，通过节点间数据同步机制保障数据的正确复制，提供数据归档工具，可以归档数据并使用传统方式备份。

同时，蚂蚁区块链通过零知识证明和数据隔离来提供隐私保护。

7. 可信执行环境与跨链技术

蚂蚁区块链基于硬件可信执行环境（TEE）提供强隐私和高性能的链上数据隐私保护服务，可以对敏感交易数据提供全链路、全生命周期的隐私保护。

蚂蚁区块链的跨链技术包括三个组成部分：UDAG 跨链协议、跨链合约服务、基于 TEE 的 Oracle 集群服务。蚂蚁区块链使用可信计算环境打造可以被外部数据调用的 Oracle 集群，解决区块链协议只能访问链上数据的局限性。

5.4.4　创建联盟链

联盟是一个虚拟组织，由多个机构组成。联盟机构可以进行以下操作：

- 共享联盟区块链；
- 创建区块链应用，并共享给联盟内的其他机构。

创建联盟的过程如下。

（1）登录控制台，选择“产品与服务”→“区块链”→“BaaS 平台”，进入 BaaS 控制台。

（2）单击“我的联盟”，如果用户当前没有联盟，可单击“添加联盟”。

（3）在“创建联盟”窗口中，选择创建类型，即“为合作商户创建联盟”或“创建自己的联盟”，然后输入联盟信息，如图 5-11 所示。

图 5-11　创建联盟链

（4）设置完毕后，单击“创建”按钮，此时联盟创建成功，“我创建的联盟”区域将显示刚

创建的联盟。

（5）联盟创建成功后，可以邀请机构加入联盟和添加联盟链。

5.5 京东 BaaS 平台

京东 BaaS 平台的网址为 https://blockchain.jd.com。

5.5.1 简介

区块链是一种新型分布式架构，以密码学和分布式技术为核心，无须借助“第三方”就能在多个业务方之间进行安全、可信、直接的信息和价值交换。在这种点对点的信息和价值交换中，区块链起到了“协议”的作用。基于这一视角，JD Chain 的目标是实现一个面向企业应用场景的通用区块链框架系统，能够作为企业级基础设施，为业务创新提供高效、灵活和安全的解决方案。

京东 BaaS 平台提供全面的“区块链即服务”功能，从企业和开发者角度出发，提供多种部署形式，既能灵活部署，又安全、易用，基于目前流行的 Kubernetes 技术，提供高可靠、可扩展的区块链平台。

京东 BaaS 平台支持企业提供集群和存储环境，支持企业自建 Baas 平台，数据完全由企业持有，从根本上解决数据安全问题。

京东 BaaS 平台提供适合于开发者的一键部署功能，可以轻松定制区块链底层和示例应用；提供适合于企业级建链的跨平台建链功能，安全方便。

通过身份链对企业证书进行透明管理，企业节点数据通过签名后完全可信，为数据交易和接口开放提供保障。基于区块链的身份认证系统为所有用户和区块链节点背书，去中心化地管理 BaaS 网络用户。

5.5.2 架构

京东 BaaS 平台充分考虑对区块链底层技术的最优封装，采用层级架构，各层级分工明确，互相协同，如图 5-12 所示。

京东 BaaS 平台提供灵活易用和可伸缩的区块链系统管理能力，无缝融合包括 JD Chain、Fabric 在内的多种区块链系统的部署管理，向企业级用户提供公有云、私有云和混合云环境的快速部署能力。

1. 资源层

京东 BaaS 平台支持企业级用户在公有云、私有云和混合云上协同部署区块链，这种跨云组网的能力使得联盟链部署更方便、灵活，通过支持多种类型的基础资源，而非捆绑在特定云平台，可提高区块链应用项目中基础设施建设的多样性，避免资源的集中导致区块链失去去中心化特征的损失。

京东 BaaS 平台基于容器编排工具调度资源，相比于裸机，具有分散调度、简化部署、提高资源利用率等优点。同时采用分布式存储系统作为区块链节点存储介质，支持海量数据存储。

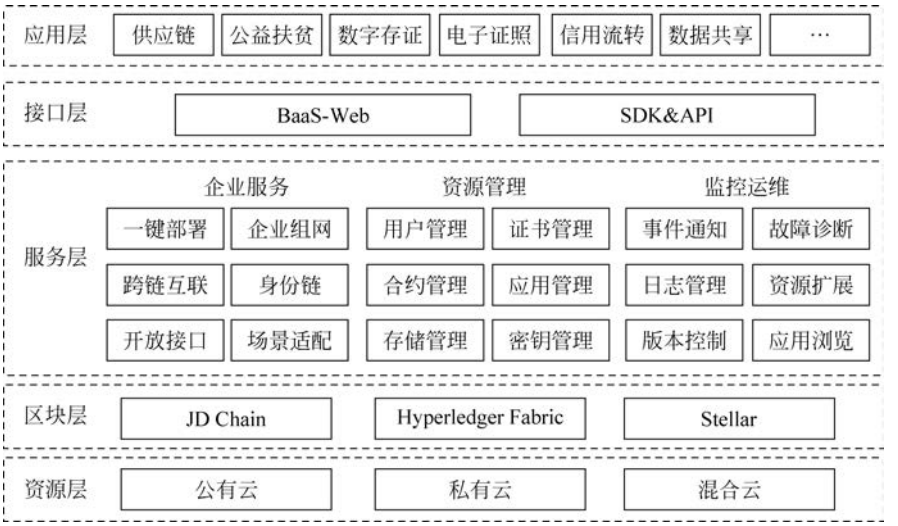


图 5-12　京东 BaaS 平台架构

2. 区块层

为满足企业对不同区块链底层技术的需要，京东 BaaS 平台支持多种区块链底层技术，供企业根据业务场景自由选择。每种区块链底层技术各有特点。JD Chain 作为京东自主研发的区块链底层，具备积木化定制等特点，适用于需要定制化高性能区块链底层的相关场景；Hyperledger Fabric 因其通用的数据存储格式，能够满足大多数企业应用的需求；Stellar 具备很强的金融属性，因此适合于金融业务场景。

3. 服务层

在区块层之上，京东 BaaS 平台依托底层区块链的支持，抽象封装了一系列服务模块。总的来说，包括 3 个种类：企业服务、资源管理和监控运维。企业服务主要帮助企业快速部署区块链技术，提供丰富功能，降低企业对区块链的入门门槛。资源管理服务主要对京东 BaaS 平台中的用户及证书进行管理，同时管理链上合约。监控运维服务在平台与区块链网络运行的过程中实时监控数据，帮助运维人员及时发现并解决问题。

4. 接口层

为满足不同用户群体的差异化需求，京东 BaaS 平台同时提供 Web 控制台和 SDK&API 接口。Web 控制台适合业务型应用场景使用，对外 API 接口采用 openAPI 标准，并提供多语言版本 SDK，可方便地将京东 BaaS 与外部系统对接。

5. 应用层

应用层通过接口层与京东 BaaS 平台解耦，基于京东 BaaS 平台提供丰富的服务接口，使得平台可以支持多种业务场景，以满足各个企业的需求。

5.5.3　特点

1. 特色服务

在京东 BaaS 平台中，各层功能相对独立，每层的内含组件各司其职，各层功能互相配合，为企业提供优质服务。其中服务层是京东 BaaS 平台的核心。

（1）区块链组网。

京东 BaaS 平台根据区块链在实际使用中的问题，为企业提供了一键部署和企业组网两种组网模式。一键部署能够帮助开发者秒级启动私有链网络，且无须关心区块链具体如何实施，只需要将关注点保持在其业务本身，降低了入门门槛。当在私有链网络中调试好业务逻辑后，企业组网模式帮助企业便捷地创建或加入生产环境的企业联盟链网络，实现业务与区块链网络快速对接。

（2）身份链。

身份链是基于区块链的身份认证系统，去中心化地认证京东 BaaS 用户，为用户和区块链节点背书。身份链的目标不是取代传统的 PKI 认证系统，相反，身份链是传统体系的信任增强，即 PKI＋区块链＝可信身份，同时也能够避免传统 CA 根密钥丢失或被盗等导致的灾难性后果。通过身份链，使身份管理透明、可信，任何接入京东 BaaS 平台的企业及开发者都能验证平台内其他用户的身份，从而提升信任度。

（3）密钥管理。

密钥的管理对所有服务平台都是较敏感的话题，如何保障数据的安全是个永恒的课题。京东 BaaS 平台的密钥管理从三个方面保证用户数据的安全。

- 信道安全：在密钥传输的过程中，API 接口强制实行 SSL/TLS 双向认证，最大程度保证传输信道安全；
- 访问安全：提供完善的访问控制策略，被策略阻挡的操作一律禁止访问，而且每次操作都会有相应的访问令牌，如令牌过期或无效都会拒绝访问，全方位保障数据访问安全；
- 存储安全：拥有完整的数据加密体系，将根私钥通过密钥分发技术分成 N 份，而需要 M 份（$N \geqslant M$）才可以解锁数据。即便数据被脱库，违法者得到的也只是加密后的数据，除非数据与 M 份密钥一同丢失。

（4）应用浏览。

主流的区块链底层技术都提供面向区块的浏览器，在数据的展示上更多的是呈现原始数据，很难与具体的应用关联起来。京东 BaaS 平台提供自研的应用浏览器（以下简称 ChainEye），ChainEye 通过支持在智能合约中内置数据展示样式，提供全网统一的、不可篡改的、符合业务规范和习惯的应用数据展示功能。

其核心内容是智能合约描述规约，规约内容涵盖智能合约的数据定义、行为定义和展示定义，这些规约内容是任何项目使用 ChainEye 来支持应用数据展示所必备的。智能合约规约的应用不仅仅局限在应用数据展示，规约本身也是业务的抽象表达。通过借助配套的辅助开发工具，能够提升智能合约的抽象层次和业务亲和性，简化智能合约代码及客户端代码的开发。

2. 设计原则

设计原则是系统设计和实现的第一价值观，从根本上指导技术产品的发展方向。京东区块链在技术规划和系统架构设计上遵循以下设计原则，如图 5-13 所示。

（1）面向业务。

“企业级区块链”的目标定位决定了系统的功能设计必须要从实际的业务场景出发，分析和抽象不同业务领域的共性需求。京东的区块链应用实践案例涉及金融、供应链、电子存

图 5-13 京东智臻链设计原则

证、医疗、政务、公益慈善等众多领域，从中获得丰富的应用实践经验，这能够为京东区块链获得良好通用性提供设计输入和业务验证。

(2) 模块化。

企业应用场景的多样性和复杂性要求系统有良好的可扩展性。遵循模块化的设计原则，可以在确保系统核心逻辑稳定的同时，对外提供最小的扩展边界，实现系统的高内聚、低耦合。

(3) 安全可审计。

区块链的可信任需要在系统设计和实现上遵循安全原则和数据可审计原则，以及满足不同地区和场景的标准与合规要求，保障信息处理满足机密性、完整性、可控性、可用性和不可否认性等要求。

(4) 简洁与效率。

简洁即高效，从设计到编码都力求遵循这一原则。采用简洁的系统模型可以提升易用性并降低分布式系统的实现风险。此外，在追求提升系统性能的同时，也注重提升应用开发和方案落地的效能。

(5) 标准化。

区块链作为一种点对点的信息和价值交换的“桥梁”，通过定义一套标准的操作接口和数据结构，能够提升多方业务对接的效率，降低应用落地的复杂度。遵循标准化原则，要求在系统设计时数据模型及操作模型独立于系统实现，让数据“系于链却独于链”，可在链下被独立地验证和运用，更好地支持企业进行数据治理，提升区块链系统的灵活性和通用性。

5.6 新华三 BaaS 平台

5.6.1 简介

Gaea 区块链平台是新华三集团技术预研部发布的一款区块链云服务平台产品，支持扩容、日志查询、API 调用、区块浏览器、跨集群设计等功能。Gaea 区块链平台旨在帮助开发者快速构建区块链基础设施，提供区块链应用开发、部署、测试和监控的整套解决方案。

Gaea 区块链平台以开发者需求为导向，底层网络基于开源架构 Hyperledger Fabric，屏蔽底层区块链的复杂部署和管理，为开发者提供简单、易用的开发者工具与区块链浏览器功能，开发者可以在可视化的操作界面下完成区块链的构建与操作，极大地降低了开发门槛和运维难度，提高了开发效率。

2018 年，Gaea 区块链平台成为全国首批通过中国信息通信研究院发起的可信区块链 BaaS 测试的平台之一，同时，用 Gaea 区块链平台创建的光模块溯源链也一次性通过了区块

链功能测试。2022 年，新华三集团成为国家级区块链基础设施“星火·链网”骨干节点技术供应商。

5.6.2 架构

Gaea 区块链平台的架构如图 5-14 所示，底层网络可以依托华三云平台，也可以直接搭建在物理服务器上，对外提供一套非常精简的 RESTful API 接口，用户业务系统可以通过这些 API 接口实现和区块链的对接，从而对外提供基于区块链的服务。

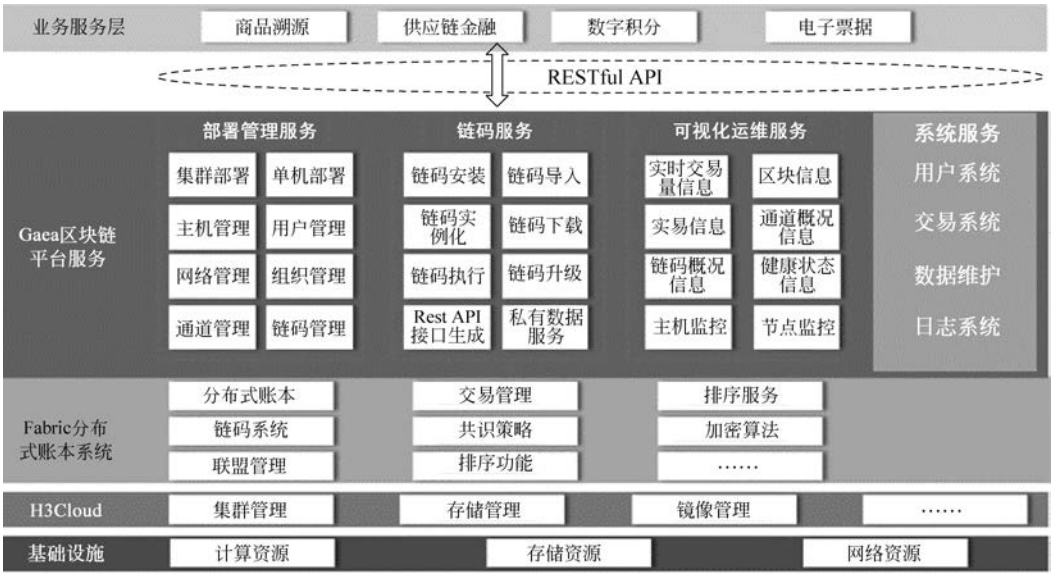


图 5-14 H3C 区块链服务的总体架构

Gaea 区块链平台可以细分为区块链网络管理、组织管理和区块链浏览器三个较大的子系统，各子系统的细分如图 5-15 所示。

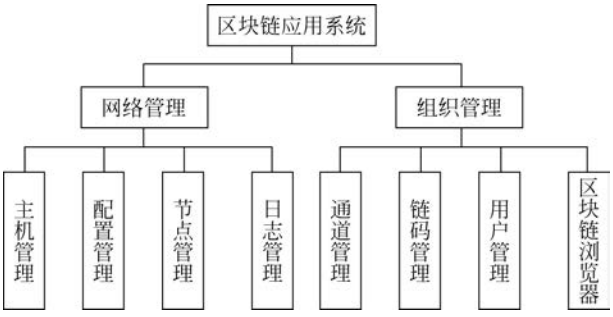


图 5-15 Gaea 区块链平台的功能架构

1. 网络管理子系统

网络管理子系统可以细分为主机管理、组织管理、节点管理、日志管理 4 部分，如图 5-16 所示。

主机管理功能主要实现区块链平台和主机的连接，主机类型可以是单机或者

Kubernetes 集群。对于单机，需要打开 2375 端口，以便实现 Docker 的管理；对于 Kubernetes 集群，需要通过 6443 端口实现对微服务的管理。主机是区块链核心 Fabric 的载体，区块链的共识、记账、查询等复杂功能都存储在主机内，当前的 Fabric 已经微服务化，各种节点都以 Docker 的形式存在。

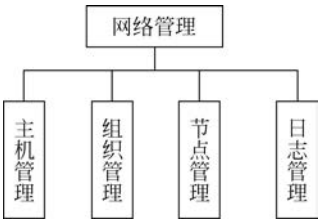


图 5-16　网络管理子系统

配置管理的功能是对区块链网络中的各组织进行配置。组织是构成区块链网络的基本单元，在一个区块链网络中必须包含两种类型的组织，分别是 Peer 类型和 Orderer 类型。Orderer 类型的组织所起的作用是为交易排序；Peer 类型的组织可以根据实际需求自行定义，一个组织可以是一个公司、机关单位或社会团体，也可以是更小规模的集体，如部门。每个组织内包含若干节点，Peer 类型的组织所包含的节点称为记账节点，区块链的区块信息就存放在记账节点内；Orderer 类型的组织所包含的节点称为排序节点，用来为每一笔交易排序。在创建组织的时候，需要选择组织所存储的主机，这样，不同的组织可以存在于不同的主机中。对于联盟链来说，联盟成员可以把自己的账本存储到自己的主机上，从而保证了账本的可靠性。

节点管理的功能是用来创建和管理区块链网络，把若干个组织组合在一起，并选择了一定的共识算法以后，就可以创建一个区块链网络。在创建的过程中会生成创世区块，并在组织所在的主机上把对应的记账和排序节点启动起来。网络还具有扩容功能，在特定的情况下，可能会根据需要，通过网络扩容功能在网络中增加新的组织。

日志管理功能主要用来记录各种操作和错误日志，在问题定位和运维过程中发挥作用。

2. 组织管理子系统

组织管理子系统可以细分为通道管理、链码管理、用户管理和区块链浏览器 4 部分，如图 5-17 所示。

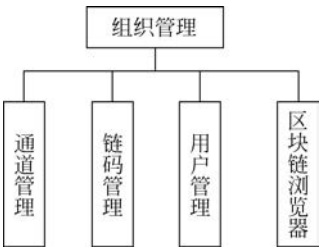


图 5-17　组织管理子系统

在 Fabric 系统中引入了通道的概念，不同的通道之间账本互相隔离，不同的节点可以选择加入不同的通道，在实现平台透明的同时，兼顾了隐私和安全性。区块链平台在通道管理功能中还实现了扩容（缩容）功能，通过邀请和批准机制解决公平性问题，每个新组织的加入（离开）必须要经过当前通道内一半以上的组织同意才能完成。

链码管理包括链码的导入、安装、实例化、升级和模拟执行等功能。在链码导入的时候，可以选择链码的语言类型，同时需要输入链码压缩包的 MD5 值，以保证正确性。链码的安装可以选择需要安装的节点。链码的实例化则可以根据需要设置背书策略。在当前链码不再适用的时候，还可以通过升级来更新链码。链码的模拟执行包括 Invoke 和 Query 两类，Invoke 的操作结果会记录到区块链中，而 Query 的结果则不会记入，这个和最终提供给用户的 RESTful API 接口保持一致，用户可以通过这两个动作验证链码的正确性。

在组织管理子系统的登录界面中，每个用户登录的同时就确定了该用户的组织信息，一旦登录，该用户只能管理自己组织内的资源，对于其他组织的资源则没有管理权限。

组织的用户管理功能可以用来创建一个本组织的管理员或者普通用户，管理员拥有本组织的所有操作权限，普通用户则只具有链码的模拟执行和一些查询功能权限，对于通道和

其他的链码操作则无权进行。

区块链浏览器可以对当前的区块链系统实现运维查看和监控，通过浏览器，可以对当前系统的实时交易量、交易信息、区块信息、通道概况和链码概况进行查看。

实时交易量监控功能：可以通过浏览器页面查看某个通道内某个节点的实时交易信息。

交易信息查询功能：可以通过交易 ID 查看某个通道内某个节点的具体交易细节。

区块信息查询功能：可以查询某个通道内某个节点的区块信息，可以进一步细分为块号查询、块数查询和时间段查询，分别是通过区块号查询某个具体的区块信息，通过区块数量查询最新的一些区块信息，通过时间段查询某一段时间内生成的区块信息。

通道概况和链码概况功能：可以监控当前系统的通道和链码的概要信息。

5.6.3 特点

Hyperledger Fabric 是目前市面上最成熟的联盟区块链系统，由 Linux 基金会主导发起，具有功能强大、性能优异、用户众多等优点，但同时存在着部署复杂、维护不便、规模受限等缺点。Gaea 区块链平台充分发挥 Fabric 系统的优点，克服 Fabric 系统的缺点，同时提供强大的运维功能，如图 5-18 所示。

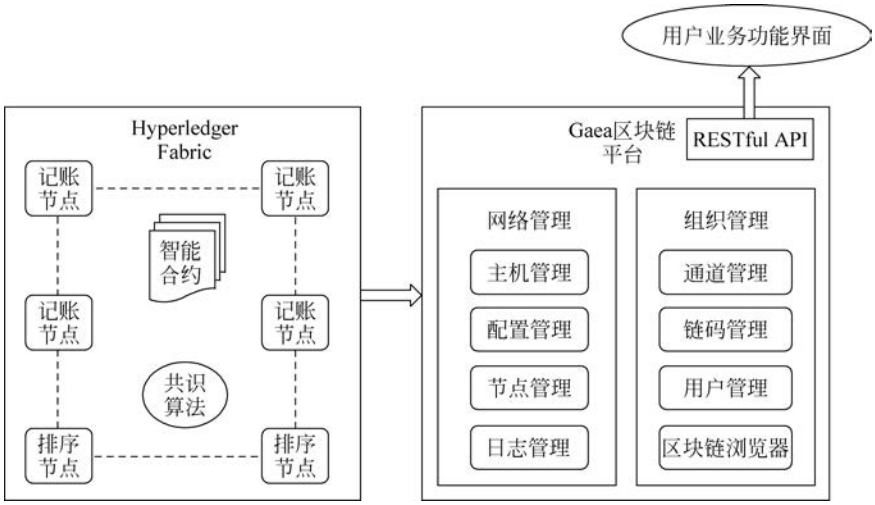


图 5-18 Hyperledger Fabric 与 Gaea 区块链平台

1. 跨主机和跨集群组网

Fabric 系统由于设计的限制，默认的组网中，一个网络中的所有组织和节点都必须在同一个主机（单机模式）或者同一个 K8S 集群中，联盟链的各个联盟成员之间并不一定是互相信任的，而在实际的工作中，大部分时候都希望自己的组织、节点、账本等运行在自己控制的主机或者 K8S 环境中，并由自己来管理。Gaea 区块链平台通过独创性的设计方案，克服了 Fabric 的默认限制，能够实现多个主机或者多个 K8S 集群联合组网，这一点对于区块链的去中心化功能非常重要。

2. 动态扩容（缩容）

Gaea 区块链平台支持动态扩容和缩容，已经创建的区块链通道由于各种原因或者环境

的变化，原有的组织规模很可能已经不再适用，这时就需要在通道中添加新的组织。Gaea区块链平台的实现方案使用了邀请的方式，通过已有的组织向新的组织发起邀请，然后，现有的组织通过签名确认来保证新组织加入的合法性，必须搜集到一半以上现有组织的签名，新的组织才能够成功加入。已有的组织如果想要离开现有的通道，也同样需要搜集一半以上的现有组织签名。该机制在保证区块链网络灵活性的同时，兼顾了安全性。

3. 专用分布式存储系统支持

区块链系统中的组织实体很多都是已有的公司或者单位，这些组织实体拥有自己的专用存储系统，在组建区块链系统的时候，会希望把账本系统存放到自己的专用存储系统中，以保证自己的账本不会丢失，Gaea区块链平台能够很好地支持分布式专用存储系统，充分利用已有的专用存储系统，并能够与K8S系统结合，实现分布式存储。另外，Gaea区块链平台还能够提供节点故障恢复功能，在记账节点故障的情况下，提供账本恢复功能。

4. 可视化管理

Gaea区块链平台上集成了区块链浏览器，区块链浏览器的基本功能包括日志管理、实时交易量查看、区块信息查看、交易信息查看、节点信息查看等，其中最重要的功能是交易信息查看和区块信息查看。交易信息查看是指通过交易ID在通道内的节点上实现具体交易信息的查看，区块信息查看是指通过区块数量查看最新一段区块信息，或者通过时间段查看某一段时间内所有的区块信息，或者通过块号查询某一个具体的区块信息。通过该功能可以直观、方便地协助运维人员来维护当前区块链。

5. 快速业务支持

Gaea区块链平台对外提供了一套非常简洁、易用的RESTful API接口，当用户把自己的业务处理链码上传到Gaea区块链平台以后，通过这套API接口，可以很容易地实现对链码功能的调用，而所有和区块链相关的复杂处理全部都由Gaea区块链平台实现，用户只需要关注自己的业务可用性和实用性。这套API接口同时还提供了用户单点登录功能，通过Token来实现安全对接。

6. 故障恢复

当记账节点发生故障的时候，可以动态检测到节点故障，并进行重启恢复，并在重启后从其他节点重新拉取账本，保证节点可靠运行；当发现K8S主机故障的时候，会在正常的主机上重启故障主机上的记账节点，并保证账本平滑地恢复；采用了基于K8S集群的分布式存储系统作为账本存储介质，充分利用集群的备份和恢复功能。

7. 平滑升级

Gaea区块链平台独立运行，版本升级不会影响区块链系统的正常工作，升级只需要简单的一键操作即可完成。Fabric版本的更新可以在保证区块链业务不中断的条件下平滑进行，通过K8S系统的服务升级能力来完成。对于已经不再适用的链码，可以通过平台的链码升级功能完成升级，保证用户业务的更新换代。

8. 多种语言链码支持

支持Go、Java、NodeJS等多种语言的链码，给用户更加灵活的选择。

5.6.4　创建区块链系统

Gaea区块链平台创建区块链系统的流程分为创建区块链网络和开展区块链业务两个

部分。创建区块链网络的流程如图 5-19 所示。

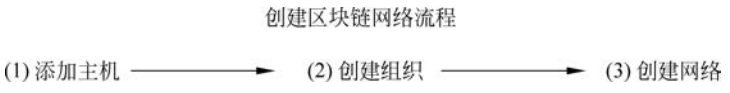


图 5-19　Gaea 创建区块链网络的流程

（1）添加主机。

主机是运行区块链网络的载体，添加主机前需要确认主机网络连接正常，确认后到主机管理页面，将目标主机添加到 Gaea 系统中。主机可以是单个服务器或虚拟机，也可以是 Kubernetes 集群。

（2）创建组织。

在组织管理中，可创建新的组织。组织分为两种类型，分别为 Peer 和 Orderer，每个网络中必须包含至少一个 Orderer 组织和多个 Peer 组织。Orderer 组织的主机（创建组织的时候会自动生成，不必单独创建）为交易排序，Peer 组织为联盟中的成员，可根据具体需求定义。在创建组织的过程中需要选择一个主机，作为该组织内节点的承载主体，后续组织内节点启动后，可以在对应的主机上查看和管理对应的节点。

（3）创建网络。

在主机和组织都准备好之后，到网络管理中创建区块链网络。网络在创建之后会自动启动，所有属于本网络组织的节点都会启动。至此，已完成了区块链网络的构建。在创建网络的过程中需要选择使用的共识协议和使用的数据库类型。

开展区块链业务的流程如图 5-20 所示。

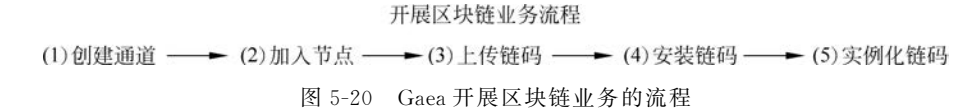


图 5-20　Gaea 开展区块链业务的流程

（1）创建通道。

通道是区块链中各组织间开展业务的载体，可以选择网络内的一部分组织来创建通道。

（2）加入节点。

在通道创建好之后，可以选择组织内的一部分或者全部账本节点，将其加入到所创建的指定通道中。

（3）上传链码。

链码是包含业务执行逻辑的代码，开展具体业务前需要将已开发好的链码上传至链码中心。

（4）安装链码。

上传完链码之后，需要将链码安装到指定的账本节点。

（5）实例化链码。

已安装好的链码需要实例化，从而实现相应业务的开展。链码实例化的过程中需要设定背书策略。

经过以上步骤，一个完整的区块链系统已经可以使用，此时用户需要调用 Gaea 区块链平台提供的 RESTful API，实现和区块链的对接。

5.7　习　　题

1. 简述 BaaS、PaaS 和 SaaS 的区别。
2. 举例说明各 BaaS 平台的应用场景。