区块链服务 BaaS

产品简介

MORE THAN JUST CLOUD | Alibaba Cloud

产品简介

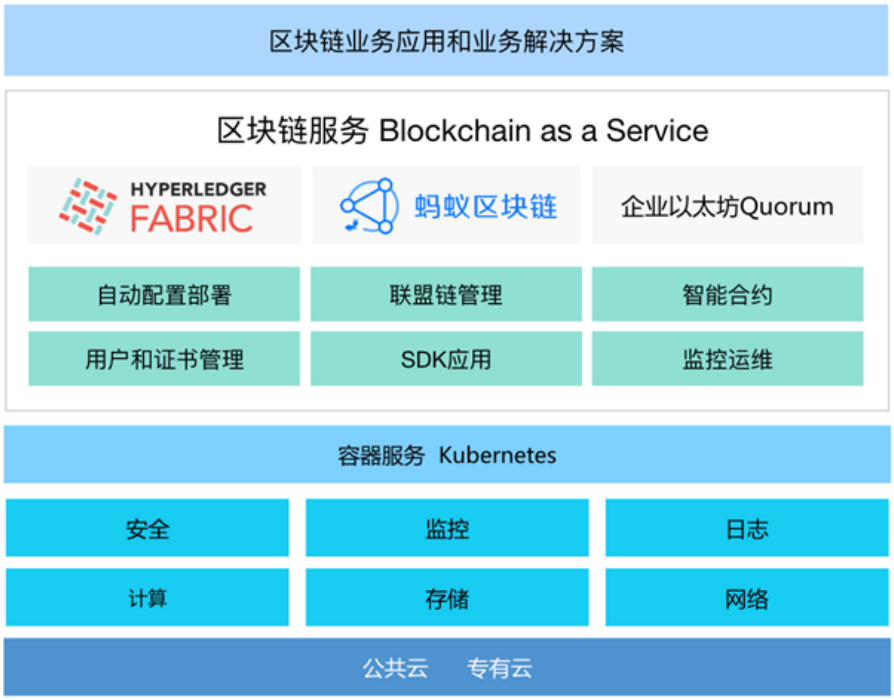
什么是区块链服务

阿里云区块链服务（Blockchain as a Service，简称BaaS）是一种基于主流技术的区块链平台服务，由蚂蚁金服区块链团队提供技术支持。它可以帮助您快速构建更稳定、安全的生产级区块链环境，大幅减少在区块链部署、运维、管理、应用开发等方面的挑战，使您更专注于核心业务创新，并实现业务快速上链。
本文从以下维度为您介绍阿里云BaaS服务：

- 为什么选择阿里云区块链服务？
- 如何使用阿里云区块链服务？
- 阿里云区块链服务API介绍

为什么选择阿里云区块链服务？

多种区块链技术引擎支持
支持主流开源区块链技术Hyperledger Fabric、企业以太坊Quorum，以及具备核心技术领先性的金融级别技术蚂蚁区块链，满足多种用户需求。



- Hyperledger Fabric，是由Linux基金会托管的开源企业级区块链技术，是开放式、标准化的区块链技术生态的代表。
- 蚂蚁区块链，是蚂蚁金服自主研发的高性能、全球部署、极强隐私保护的金融级联盟区块链技术。
- 企业以太坊Quorum，是摩根大通（J.P. Morgan）基于以太坊开发的面向企业场景、符合EEA（Enterprise Ethereum Alliance）规范的开源企业级区块链技术。

一键式部署

阿里云区块链服务帮助用户一键式快速创建和部署生产级区块链环境，提供图形化的区块链管理运维能力，实现参与企业和业务的动态添加，简化区块链的部署流程和应用配置。

隔离性

基于阿里云区块链服务创建的联盟链网络，建立在云计算多租户隔离（包括计算/存储/网络等资源的隔离）的基础之上，保证了区块链业务参与方的独立性和自治性。

跨地域

业务参与方可分布于不同的地域，实现跨地域联盟网络的建立。例如，如下图所示，联盟链网络中的各方（运营方和参与方）可以分别部署于三个不同的城市。

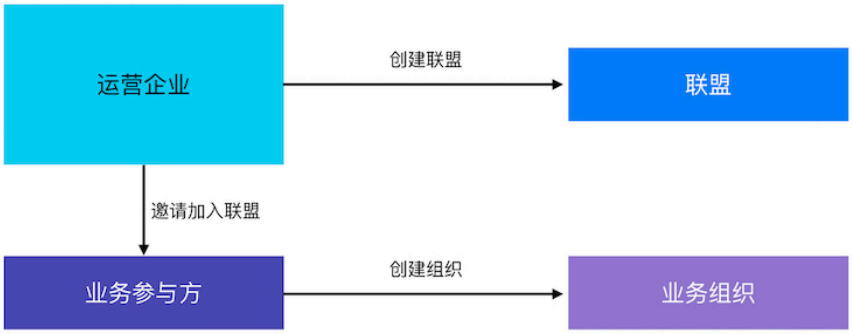
阿里云BaaS服务还提供了广泛的接入方式、动态的资源创建和弹性可扩展能力，以及多维度的安全和隐私保护机制，同时在成本上也具备更灵活的优势。 更多阿里云BaaS优势请参见 产品优势 章节。

如何使用阿里云区块链服务？

基于Hyperledger Fabric、蚂蚁区块链的阿里云BaaS服务已商用，企业以太坊Quorum的BaaS服务目前正火热公测中。

Hyperledger Fabric

由运营企业创建联盟，各个业务参与方创建组织。然后运营企业邀请各个业务参与方加入联盟以及对应的业务通道。在这种模式下，联盟的基础设施运营由一家受委托的企业负责，其他参与方作为进行业务协作和交易的角色共同参与。运营企业自己也可作为参与方创建组织，进而加入联盟及通道。



使用流程

1. 开通服务。
   您可以在BaaS产品首页，参考选购指南章节开通BaaS服务。

   创建区块链网络

进行创建组织、创建联盟、组织加入联盟、创建通道的操作。具体请参见使用流程。

部署链码

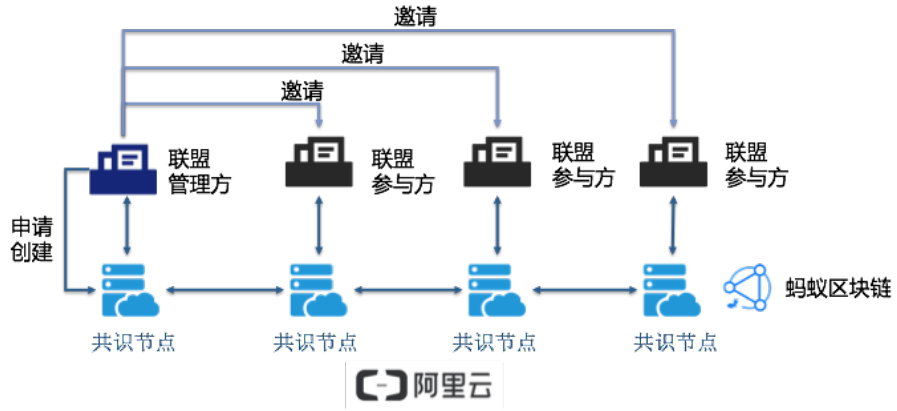
包括上传链码、安装链码、实例化链码的操作。具体请参见部署链码。

访问区块链网络

包括创建用户和通过SDK访问区块链网络。

蚂蚁区块链

蚂蚁区块链使用模式如下图所示。



联盟管理方发起申请联盟链创建，然后邀请其它联盟参与方加入。联盟参与方接受邀请加入联盟后，对联盟链的共识节点进行访问、读写，具体的使用流程如下。

1. 开通服务。
   您可以在 BaaS 产品首页，参考 选购指南 章节开通 BaaS 服务。

   申请区块链

   您可以在控制台，申请加入区块链或者申请创建联盟链。具体请参见 管理联盟区块链。

   管理区块链

   进入控制台管理页面后，您可以邀请其它用户加入您的联盟链，审核其他联盟方加入的申请，管理节点，查看区块链详情等操作。具体请参见 创建联盟。

   访问区块链网络

   通过 开发指南，访问区块链网络。

企业以太坊Quorum

1. 开通服务。
   您可以在 BaaS 产品首页，参考 选购指南 章节开通 BaaS 服务。

   创建区块链网络

   您可以在控制台创建企业以太坊Quorum区块链网络。具体请参见创建一个区块链网络。

   管理区块链

   您可以邀请阿里云用户参与到Quorum区块链网络中，然后添加来自于阿里云BaaS的Quorum节点，具体请参见邀请阿里云BaaS用户加入和添加来自阿里云BaaS的节点；也可以直接添加来自于其他云平台（如AWS、Azure）或者私有部署环境的Quorum节点，具体请参见添加外部节点。

   部署智能合约

   在完成智能合约的开发后，您可以编译和部署智能合约，以及发送交易调用智能合约，具体请参见使用solc编译智能合约、使用geth部署智能合约和使用geth发送交易。

阿里云区块链服务API介绍

阿里云区块链服务API在区块链底层技术原生API之上进行了扩展，支持对区块链服务相关的区块链对象和云资源对象的操作，并简化了原生API对区块链服务的管理、运维、调用等复杂过程，使得用户可以方便地通过API对区块链联盟、组织、节点、通道、智能合约、底层资源、日志、配置信息等对象进行管理和维护。

区块链服务API支持HTTP和HTTPS请求，同时要求使用阿里云账户生成的Access Key和Access Key Secret进行身份验证，以保证API调用的安全性。

此外，您还可以通过阿里云OpenAPI Explorer, 以图形化网页方式，快速检索和可视化调试区块链服务的API。

如需了解和开始使用区块链服务API，请参见API参考。

产品优势

Hyperledger Fabric

开放共享

- 基于主流开源区块链技术Hyperledger Fabric，原生支持符合Hyperledger Fabric标准的区块链应用和数据；代码开发成果持续贡献开源社区，保证技术的开放透明性。
- 未来将整合更多优秀的区块链技术体系，为用户打造一个开放共享、能力全面、标准统一的区块链应用生态圈。

高安全

- 支持基于国密算法的加密、解密。
- 内建面向多企业联盟链的治理体系，确保企业间协作流程的可控和可信。
- 为业务参与方提供多维度的网络隔离、网络访问控制与攻击防护。
- 各参与方拥有独立的CA服务，满足企业独立证书体系的需求。
- 内置风控和操作审计功能，无惧“乌龙指”风险。

高可用

- 系统全链路实现高可用设计，包括区块链节点、服务管控、容器集群、云基础资源等，确保业务连续性。
- 区块链账本数据的底层存储具备极高的可靠性（99.999999999%），并能在应用无感知、无中断的前提下实现存储弹性扩容。

简单易用

- 一键式操作，快速获得完整的企业级区块链网络。
- 提供图形化、丰富的管理运维功能，帮助用户轻松配置、部署、管理、监控企业所拥有的多个区块链网络，并且无需精通区块链底层技术细节，降低区块链使用门槛，减轻技术复杂性带来的痛苦。
- 提供区块链应用开发REST API，SDK 以及BaaS VSCode插件，大大降低了开发者的门槛。
- 与函数计算，MQ，内容安全等云服务深度集成，为用户提供了便捷的链上链下协同功能，帮用户省去了区块链与其它服务的集成开发成本。
- 避免企业在底层区块链和基础资源的建设和运维等方面过多的投入，让企业专注于区块链之上的业务应用创新。

高性能

基于阿里云的高性能云服务器、高带宽网络、高并发高吞吐的存储技术，释放区块链的性能潜力。

全球部署

- 阿里云的数据中心广布全球，助力用户实现业务系统的全球化部署。
- 基于阿里云成熟的海外合规流程和最佳实践，确保业务系统的安全合规运行。

蚂蚁区块链

作为行业领先的区块链服务平台，蚂蚁区块链 BaaS 平台具备以下优势：

高性能

金融科技区块链基于全球领先的并行共识技术，轻松满足金融领域的高频场景应用。

高可靠性

业务可靠受理，峰值业务缓冲，基于 PBFT 的共识技术提供高可用的拜占庭容错能力，支持共识状态自动恢复，区块数据互备恢复，数据存储自动均衡，节点服务自动路由。

双重权限信任保护

提供双重权限信任保护。第一重，联盟链的可信参与方对该联盟链可见，其它用户对该联盟链不可见；第二重，参与联盟链须提交用户 CA 证书申请并等待审核，通过审核后方可参与联盟链操作。

跨网络部署

可以根据联盟参与方需求跨云平台部署区块链节点，即部分参与共识的节点运行在阿里云平台，部分参与共识的节点运行在用户的 IT 环境。

数据隐私及安全

用户可以选择明文数据上链，也可以对称加密的方式对上链数据进行加密。同时支持分享隐私模型，即将加密密钥通过另一把私密密钥加密，加密后的明文和加密后的密钥上链保存。私密密钥通过特定的密钥导出函数进行管理，根据不同安全级别和分享范围分享不同的私密密钥。

简单易用

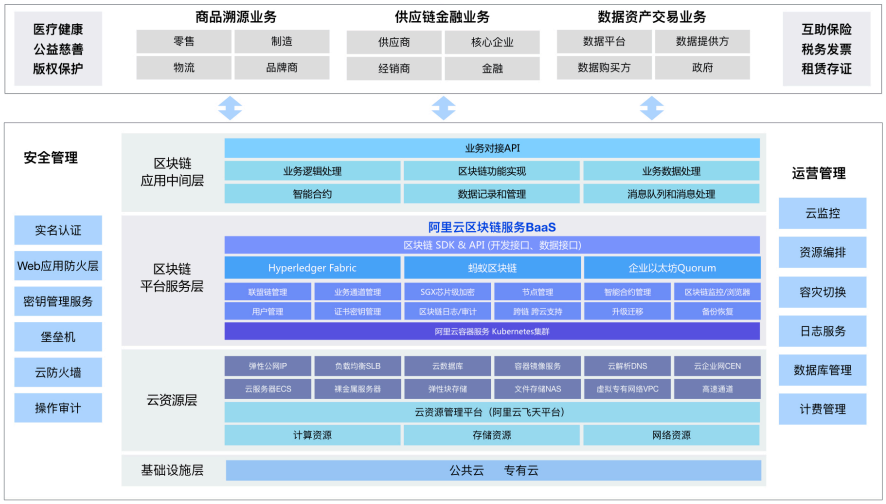
减小区块链使用门槛，用户无需精通或掌握区块链底层技术细节，无需相关的资源环境运维投入，从而使用户专注于基于区块链技术的业务应用和场景的创新与开发。

产品架构

阿里云区块链服务构建于Kubernetes之上，支持业界主流的区块链引擎技术，与阿里云丰富的云服务进行整合，支持用户构建跨企业、跨地域的业务协作和交易网络，实现区块链业务场景的快速落地。

产品功能架构

- 基础设施层：支持公共云、专有云（敏捷版）等部署形态，未来进一步支持混合云部署形态。
- 云资源层：包含区块链服务及上层应用所需要的云基础资源，包括ECS、VPC、NAS、SLB等等。
- 区块链平台服务层：构建于阿里云容器服务Kubernetes集群之上，实现了资源创建、管控运维、安全治理等BaaS基础服务，区块链引擎支持Linux基金会旗下Hyperledger Fabric（1.4 LTS），蚂蚁金服旗下的蚂蚁区块链，以及J.P. Morgan旗下的企业以太坊Quorum。
- 区块链应用中间层：此为参考架构，主要实现BaaS与业务的对接，一般通过区块链业务解决方案或区块链中间件等形式实现。
- 整体架构还包括区块链服务与业务应用可能用到的安全管理、运营管理等各项云服务。



应用场景

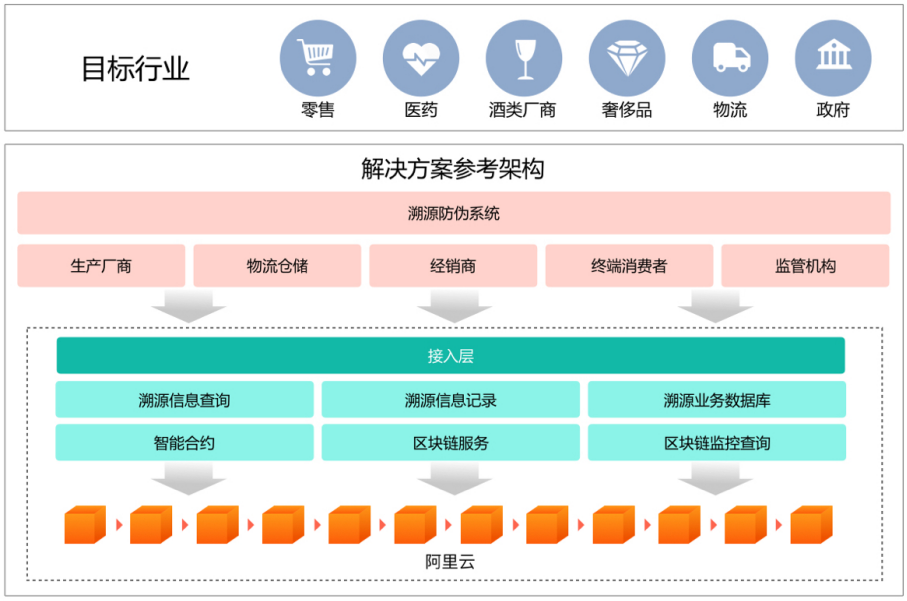
应用场景

阿里云区块链服务BaaS可应用于各大行业的多种业务场景中，例如：商品溯源、数据资产交易、供应链金融、数字内容版权、公益慈善、信用证、资产证券化、资产托管、能源化工交易、房产交易租赁、数字身份等。下面以其中两种场景为例进一步说明。

商品溯源场景

在传统的商业零售场景中，商品从出厂到消费者的链条存在中间环节信息不透明的情况。当发生商品质量或安全问题时，难以回溯和追责。同时供应链信息也存在被篡改或伪造的风险。

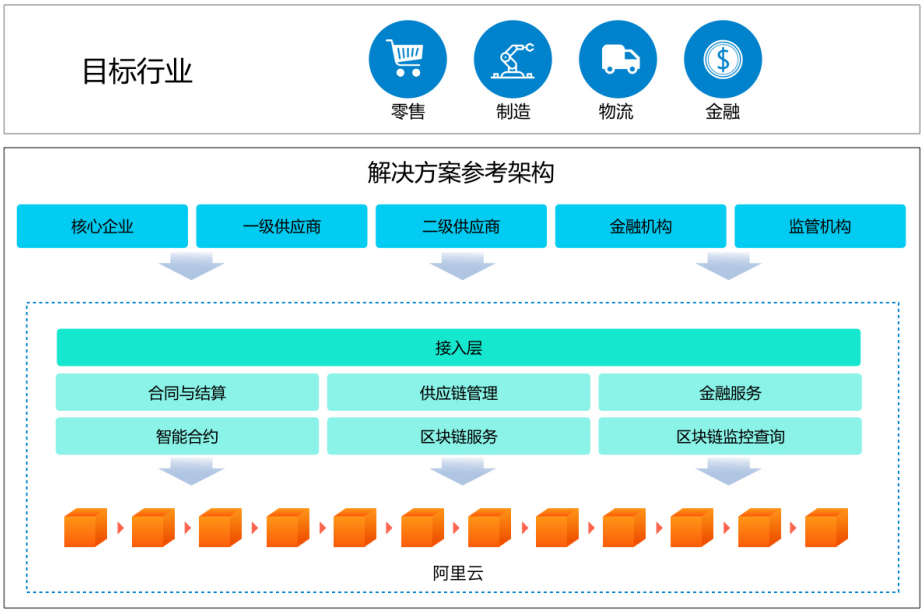
区块链在其中起到的作用是，可以实现多方共同记录溯源信息，让消费者可对商品实现溯源查询和验真。同时，区块链保证了溯源信息是经过各个业务参与方共同确认的，具备不可篡改性。区块链上的全流程交易历史记录均可被审计，满足政策和监管的要求。此外，区块链需要结合适用于各种商品形态的防伪以及数字化技术，才能形成一套完善的溯源方案。



供应链金融场景

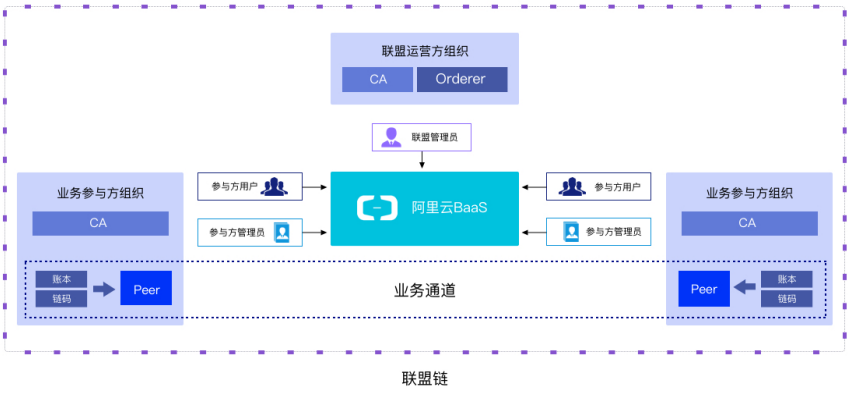
在传统供应链体系中，除了核心企业外，还包含了上游的多级供应商和下游的多级经销商，但由于企业的信用无法实现传递，导致许多企业面临融资难、融资慢的问题，影响了业务的健康发展和生产规模的扩大。同时由于信息难以共享，使得企业间交易协作的效率较为低下，比如由于票据流通不便导致的合同结算慢的问题。

区块链可以实现核心企业的应收应付等信息在供应商、经销商、金融机构间流转，传递企业的信用，帮助参与企业解决融资方面的难题。区块链在实现这些企业之间共享交易数据的同时，可有效保护商业隐私和信息安全。此外，区块链的智能合约可实现企业债券流转、资金自动清算，加速企业的业务运作和资金流转的效率。



使用模式

Hyperledger Fabric使用模式



区块链服务为Hyperledger Fabric提供了两种使用模式。企业用户在使用区块链服务用于各种业务场景的时候，可根据实际情况和需求选择合适的使用模式。

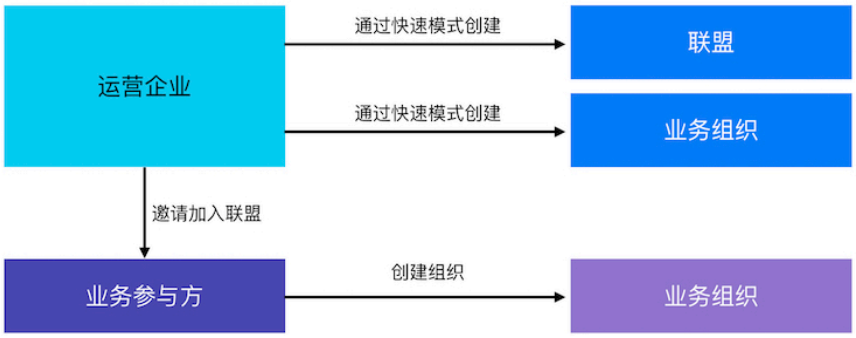
注：以下信息仅供参考。两种使用模式之间并没有严格的界限，用户可根据需要灵活地选取。

快速模式

如果业务联盟是由一家核心企业发起或主导的，其他业务参与企业是受其邀请进入的，那么可考虑采用快速模

式。

快速模式可以让核心企业快捷地开始基于区块链的业务，然后在后续阶段逐步添加更多的业务参与方进入联盟链和业务通道。在这种模式下，核心企业兼具了联盟运营方和业务参与方的角色，其他企业均作为业务参与方

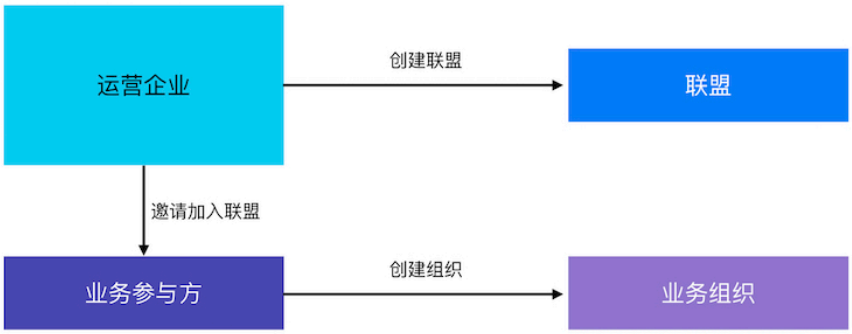


。

常规模式

如果业务联盟的基础设施运营由一家受委托的企业负责，其他企业作为真正进行业务协作和交易的角色共同参与，那么可以采用常规模式。

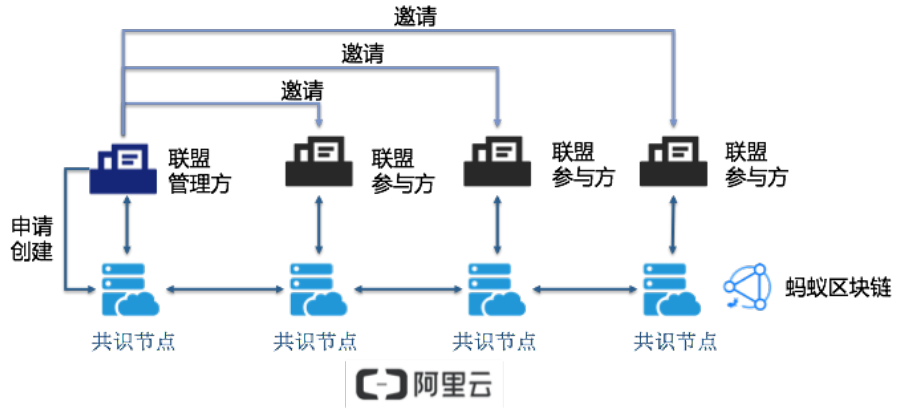
常规模式下，由运营企业创建联盟链，然后运营企业邀请各个业务企业加入联盟链以及加入对应的业务通道。在这种模式下，运营企业担任了联盟运营方的角色（但不属于业务参与方），而业务企业则作为业务参与方的



角色。

蚂蚁区块链使用模式

蚂蚁区块链使用模式如下图所示，联盟管理方发起申请联盟链创建，然后邀请其它联盟参与方加入。联盟参与方接受邀请加入联盟后，对联盟链的共识节点进行访问、读写。



基本概念

通用概念

比特币

英文名称Bitcoin，由中本聪于2008年提出的一种电子加密货币，在全球具有很高的知名度，是区块链早期的典型应用。

区块

英文名称Block，每个区块记录着上一个区块的hash值、本区块中的交易集合、本区块的hash等基础数据。由于每个区块都有上一区块的hash值，区块间由这个值两两串联，形成区块链。

区块链

英文名称Blockchain，最早起源于比特币的底层技术，并在其后不断演进发展。区块链本质是一种多方共享的分布式账本技术。它通过数学方法实现交易数据和历史记录的不可篡改性，通过共识算法和智能合约实现各参与方对交易的共同确认和账本记录。区块链分为公有链、联盟链、私有链三种基本类型。区块链的实现技术框架有以太坊、EOS、Hyperledger Fabric、Corda等等。

智能合约

区块链技术的特性之一，用计算机语言描述合同条款、交易的条件、交易的业务逻辑等，通过调用智能合约实现交易的自动执行和对账本数据的操作。

证书颁发机构

英文名称Certificate Authority，简称CA，数字证书颁发机构是受信任的第三方机构，颁发的数字证书是为最终用户数据加密的公共密钥。

交易

英文名称Transaction，区块链接收的数据称之为交易。

区块链高度

Height，当前区块链上出块（Block）的最大数目

哈希

Transaction Hash同交易哈希。交易上链成功后，产生的唯一哈希值

Hyperledge Fabric特有概念

联盟

区块链专业术语，英文名称consortium，指参与一个基于区块链的业务协作或业务交易网络的所有组织的集合，一个联盟一般包含多个组织。

在阿里云区块链服务（Hyperledger Fabric）中，每个联盟需要有一个联盟实例，一般由联盟发起方或运营方创建，该实例包含Orderer排序节点，负责交易排序、区块产生和达成共识。联盟运营方邀请各个组织实例加入联盟，进而创建通道，并负责Orderer排序节点的管理运维。

组织

区块链专业术语，英文名称organization，代表的是参与区块链业务网络的企业、政府机构、团体等实体。在阿里云区块链服务（Hyperledger Fabric）中，一个组织实例主要包含如下节点：

- CA：区块链节点类型之一，英文名称Certificate Authority，数字证书颁发机构，负责组织内部成员的register和enroll等，为该组织的区块链用户生成和颁发数字证书。
- Peer：区块链节点类型之一，负责保存和记录账本数据、对交易背书、运行智能合约等。

在阿里云区块链服务（Hyperledger Fabric）中，一个区块链网络由 1个联盟实例 + N个组织实例构成，N>=1。组织实例的个数 N 由业务参与方的个数以及是否有独占需求决定。如果参与方需要独享的区块链节点和账本，以及链码部署，区块链用户创建等管理功能，则需要单独创建一个组织实例。如果参与方对独占没有要求，则可以共享组织实例。联盟实例和组织实例可以由单一的云账号购买创建，也可以由不同的云账号购买创建。

通道

区块链专业术语，英文名称channel，主要用于实现联盟链中业务的隔离。每个通道可代表一项业务，通道内包含业务的参与方（联盟内的部分或全部组织）作为通道成员。一个联盟中可以有多个通道；一个组织可以加入多个通道。每个通道可视为一条子链，并且对应一套账本，通道上可发布智能合约。

链码

区块链专业术语，英文名称chaincode，是Hyperledger Fabric技术框架中对智能合约的实现，支持业界流行的编程语言如Node.js、 Go、Java等。

Orderer

区块链专业术语，排序节点，指的是Hyperledger Fabric技术框架下提供共识服务的节点，区块链网络内所有交易在完成背书后会被发送至Orderer节点进行排序，然后根据一定的规则生成区块，并向区块链网络上的Peer节点发送区块以进行区块和交易的验证并写入账本，从而完成共识的全过程。

Peer

区块链专业术语，参与方节点，指的是Hyperledger Fabric技术框架下，业务参与方组织在区块链网络中所拥有的参与共识和账本记录的节点。分为两种类型：Endorsing Peer，背书节点，必须安装链码，在交易时需进行签名背书；Committing Peer，记账节点，无需安装链码，只负责验证从Orderer发出的区块和交易的合法性、并存储账本区块信息。

Anchor

区块链专业术语，锚定节点，指的是Hyperledger Fabric技术框架下，为了实现高可用，每个参与方组织包含两个或多个peer节点，设置其中的一个为anchor，与区块链网络中的其他组织进行信息同步。

蚂蚁区块链特有概念

参与角色

分为两种：

- 联盟管理方，负责发起申请联盟链创建，拥有联盟链的管理权限，可以邀请其它联盟参与方加入。
- 联盟参与方，对联盟链有独立的访问、读写权限。

存证数据

英文名称Ledger Data。区块链本身具有不可篡改的特性，写入区块链的数据都是可信任、不可篡改的，为了让数据具备公正力，写入区块链的数据可称为存证数据，存证数据可以为一个字符串、一个文件的hash等，以表示文本、文件等存证数据。

证书申请

英文名称Certificate Signing Request。证书签名请求文件（CSR，Certificate Signing Request），通过openssl等工具生成。生成过程中会产生2个密钥，一个是公钥就是这个CSR文件，另外一个是用户私钥，用户需保存好私钥和私钥密码。

私钥

英文名称Private Key。私钥文件，通过openssl等工具生成。生成过程中会产生2个密钥，一个是公钥是证书签名请求文件，另外一个是用户私钥，用户需保存好私钥和私钥密码。

签名证书

英文名称Certificate。由支付宝合作的第三方CA机构根据用户提交的证书请求签发认证后的证书。

专有区块链

英文名称Private and Consortium Blockchain。用户申请由自己使用的或管理的区块链。

节点信息

英文名称Node Information。区块链节点的相关信息。一个区块链一般由多节点组成，节点数目为3f+1/其中f为正整数。

业务分类

英文名称Business Classification。该交易上链的数据的业务数据格式类型。

引用个数

英文名称Reference Count。该交易是否引用了其它交易。

业务时间

英文名称Business Time。该交易的提交生成时间。

企业以太坊Quorum特有概念

以太坊虚拟机

英文名称Ethereum Virtual Machine，简称EVM。以太坊平台的核心组成部分之一，作为运行智能合约的分布式计算环境。

Solidity

Solidity是一种高层的智能合约编程语言，语法类似JavaScript，用于编写可运行于以太坊虚拟机内的代码。

Gas

用来衡量一笔交易所消耗的计算资源的基本单位。当以太坊节点执行一笔交易所需的计算步骤越多、越复杂，那么这笔交易消耗的Gas就越多。

网络标识

英文名称network id。用于代表特定版本的以太坊网络的数字标识。

geth

以Go编程语言实现的以太坊客户端。

Dapp

分布式应用。

私密交易

英文名称Private transaction。交易载荷信息仅对指定的区块链网络参与方可见，通过在交易的privateFor参数中指定这些参与方的公钥来实现。

Quorum节点

英文名称Quorum node。在geth的实现基础上包含如下的修改：

- 支持Istanbul BFT、RAFT等共识算法；
- 支持授权节点（permissioned node）的P2P层实现；
- 私密交易的区块验证逻辑；
- 保留了Gas机制但移除了Gas价格。

交易管理模块

英文名称Transaction manager。Quorum的交易管理模块主要用于支持交易私密性。它存储了加密的交易数据，提供授权访问，与其他参与者的交易管理模块进行加密数据的交换（同时不会接触任何敏感的私钥）。交易管理模块通过Enclave调用加密相关功能。交易管理模块采用RESTful和无状态设计，易于实现负载均衡。

Enclave

Enclave与交易管理模块进行协同工作，共同支持隐私交易。Enclave独立负责加密和解密工作并保存私钥，为

Quorum其他组件提供一种类似虚拟HSM的服务。

云服务集成

阿里云区块链服务能够集成其他云服务并提供链上链下协同的便捷功能，减少区块链底层与其它云服务集成的开发成本，帮助您快速完成系统构建。

函数计算

当您希望区块链上的各种事件能自动触发链下业务逻辑时，您可以在阿里云函数计算服务中上传业务逻辑代码，并在云服务集成中将区块链事件和函数代码做映射配置。当链上发生您配置监听的事件时，事件会被自动推送到您配置的函数中，触发您的业务逻辑代码。操作步骤可以参考**集成函数计算**，详细示例可以参考**链上事件触发链下操作**。

消息队列 RocketMQ

通过集成消息队列 RocketMQ服务，云服务集成会根据配置，将区块链上的事件可靠、自动地发布到消息队列RocketMQ的特定主题上，其它应用可以订阅MQ中的这些事件消息，做进一步的处理。操作步骤可以参考**集成消息队列**，详细示例可以参考**链上事件发送到消息队列**。

外部 HTTP 服务

通过集成外部 HTTP 服务，可以让区块链上的各种事件自动触发您的自有业务应用或者第三方服务，并将事件内容推送到外部做进一步加工处理。操作步骤可以参考**集成外部HTTP服务**。

内容安全检查

由于区块链的不可篡改特性，如果链上数据存在违法违规信息，则难以单独清除。通过集成阿里云内容安全服务可以防范此类问题，避免违法违规信息上链。操作步骤可以参考**集成内容安全**，使用示例可以参考**数据合规上链**。

数据库

区块链上的数据一般以key-value形式存储，不方便做数据查询及分析。通过集成关系型数据库，云服务集成会根据配置，将链上数据可靠、自动地导出到目标数据库的特定表格里，其它应用可以通过SQL语句，分析工具做进一步的处理。操作步骤可以参考**集成数据库**，使用示例可以参考**链上数据导出到数据库**。

对象存储OSS

阿里云区块链服务支持将大容量数据或文件存储于对象存储OSS，同时通过可信手段与区块链的链上数据进行关联，保证原始数据和文件内容的可信和不可篡改。阿里云区块链服务提供了一个示例程序可供参考。

视频DNA

阿里云区块链服务支持与视频DNA服务进行融合，通过视频DNA技术对多种媒体(图文、视频、音频等)进行唯一标记，依托区块链将DNA等关键信息上链，进而构建拥有版权存证、侵权追溯和版权交易等能力的平台。详情可参考区块链版权保护解决方案主页。

云企业网（CEN）和云解析PrivateZone

阿里云区块链服务支持与云企业网（CEN）以及云解析PrivateZone构建基于混合云的联盟链网络。云企业网为区块链服务在VPC之间、VPC与本地数据中心之间实现区块链节点以及应用的安全互通，同时基于云解析PrivateZone实现在安全联盟链网络环境内的区块链服务私有域名解析和管理能力。

Link TEE

阿里云区块链服务企业版和企业安全版支持在Link TEE（物联网可信执行环境）运行Hyperledger Fabric Client SDK（私钥管理和签名），可为区块链应用提供更强的安全防护，特别是保护物联网（IoT）场景中运行于边缘设备上的区块链应用。详情可参考企业级区块链服务-IoT边端安全方案。

DDoS防护

阿里云区块链服务已内置整合DDoS基础防护服务，同时可支持更高防护级别的DDoS防护包、DDoS高防IP，满足对核心关键业务的抗DDoS攻击需求。

如需了解阿里云区块链服务与上述云服务整合的方案细节，可通过工单形式联系阿里云支持团队。