

蚂蚁链 区块链平台

BaaS产品白皮书

目录

0. 目的	2
1. 产品概述.....	2
1.1 背景.....	2
1.2 产品定位.....	3
1.3 产品优势.....	4
2. 产品架构.....	5
2.1 业务场景.....	5
2.2 产品核心架构.....	6
2.3 产品功能简介.....	6
2.3.1 BaaS 平台核心能力	6
2.3.2 BaaS 平台增值服务能力	6
3. 应用场景.....	8
3.1 政务场景.....	8
3.2 供应链金融.....	8
3.3 溯源场景.....	8
3.4 数字资产流向分析.....	8
4. 产品功能.....	9
4.1 BaaS 平台核心能力	9
4.1.1 控制台功能.....	9
4.1.2 区块链开发	17
4.1.3 智能合约开发.....	21
4.1.4 链底层能力.....	24
4.2 BaaS 平台增值服务能力	35
4.2.1 数据洞察能力.....	35
4.2.2 跨链连接服务（ODTAS）	37
4.2.3 一体化服务平台.....	40

4.2.4 多链综合管理平台.....	41
4.2.5 多方协同存储.....	42
4.2.6 区块链传输网络（BTN）.....	43
5. 典型案例.....	46
5.1 案例一：浙江省电子票据管理中台.....	46
5.2 案例二：浙商中拓工程配送项目.....	47
5.3 案例三：GSBN 无纸化放贷项目	48

0. 目的

本白皮书旨在帮助政府、企业及社会组织的技术和业务团队了解如何利用我们的区块链服务（BaaS）平台，快速、安全地构建和部署分布式应用。通过深入解析平台架构、功能特性及典型应用场景，展示了如何通过 BaaS 平台，实现更多业务价值和更高效的跨组织合作。白皮书深入探讨了本产品如何结合区块链技术、隐私保护技术、跨链技术和高速传输网络，在大规模组网下，实现链上数据及数字资产在跨组织业务场景中的可靠、安全、快速地流转，进一步释放数据价值。

1. 产品概述

1.1 背景

随着信息技术的迅猛发展，区块链技术作为一种颠覆性的技术逐渐进入大众视野。区块链，最早因其在比特币等加密货币中的应用而广为人知，近年来逐渐扩展应用领域，并在供应链管理、金融服务、医疗健康、物联网等多个行业展示了其独特的价值。

区块链是一种分布式的数据库技术，通过共识机制、加密算法和智能合约等技术手段，实现了去中心化的可信计算。自 2008 年比特币白皮书问世以来，区块链技术经历了多个发展阶段。从早期的加密货币时代，到以太坊引入智能合约，再到如今的多种区块链技术并存、跨链技术蓬勃发展的局面，区块链技术已成为数字经济的重要组成部分。

在信息化快速发展的今天，数据已成为新的生产要素。然而，由于传统集中式数据存储和处理模式存在数据泄露、篡改、单点故障等安全隐患，企业在进行数据共享和业务协作时面临诸多挑战。区块链技术的去中心化、不可篡改和高透明性特性恰好能够满足现代社会对数据安全和隐私保护的需求。

此外，传统的中心化信任机制效率低下、成本高昂，通过区块链去中心化的共识机制，能够在多方协作中重构信任关系，实现业务流程的透明与可追溯性。因此，越来越多的企业开始探索如何将区块链技术应用于实际业务场景，以提升其运营效率和竞争力。

近年来，区块链技术在性能优化、隐私保护、智能合约和跨链技术等方面取得了显著进展。新的共识算法（如 PBFT、ABFT 等）在提高共识效率和降低能源消耗方面展现出巨大潜力。隐私保护技术如零知识证明和环签名，在保证数据隐私的前提下实现了数据的公开验证。

跨链技术的发展，使得不同区块链之间的数据和资产流转成为可能，打破了区块链孤岛问题，实现了更加广泛和灵活的应用。同时，高速传输网络（BTN）技术在大规模组网下提供了快速、可靠的数据传输解决方案，进一步提升了区块链网络的性能和稳定性。

在上述行业背景和市场需求的推动下，我们的区块链服务（BaaS）平台应运而生。本产品旨在解决企业在跨组织合作中面临的数据安全、隐私保护和高效传输等问题，促进数据和资产的流转，释放数据价值。通过结合区块链技术、隐私技术、跨链技术和高速传输网络，本产品在大规模组网下，实现了链上数据在跨组织业务场景中的可靠、安全、快速流转。

1.2 产品定位

区块链 BaaS（Blockchain-as-a-Service）平台依托蚂蚁链平台开放行业领先的金融科技区块链服务。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开发、测试、上线，助力各行业区块链商业应用场景落地。提供高性能，稳定可靠，隐私安全，多种类型数据的区块链存证能力。

我们的区块链服务（BaaS）产品定位于提供安全、高效、易用的区块链解决方案，旨在帮助各类组织快速构建和部署分布式应用，实现数据的可靠与高效流转，并推动多方协作的数字化转型。我们面向的客户包括但不限于：

- **政府机构：**满足政府在数据管理、公共服务、电子政务等方面的需求，通过区块链提升数据透明性和公共服务效率。
- **大型企业：**支持金融、制造、医疗、物流等行业的大型企业，解决跨部门、跨组织的业务协作问题，优化供应链管理，提升运营效率。
- **中小企业：**帮助中小企业快速构建区块链应用，降低技术门槛，实现业务创新和数字化转型。
- **社会组织：**为非营利机构、社会团体提供透明的管理工具，提升信息公开和业务管理的透明度。

1.3 产品优势

与市场同类产品相较而言，蚂蚁链 BaaS 平台具有以下几点特色和优势：

- **高性能：**蚂蚁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，联盟链对可信参与方可见，对其它用户不可见；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金融科技平台，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。
- **网络安全保障：**多个独立的区块链节点部署在金融区的 VPC 网络中，保证网络安全性。同时，该 VPC 网络与用户在金融科技平台上的 VPC 可以连通，保证用户应用在安全的网络环境中访问操作区块链。
- **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。

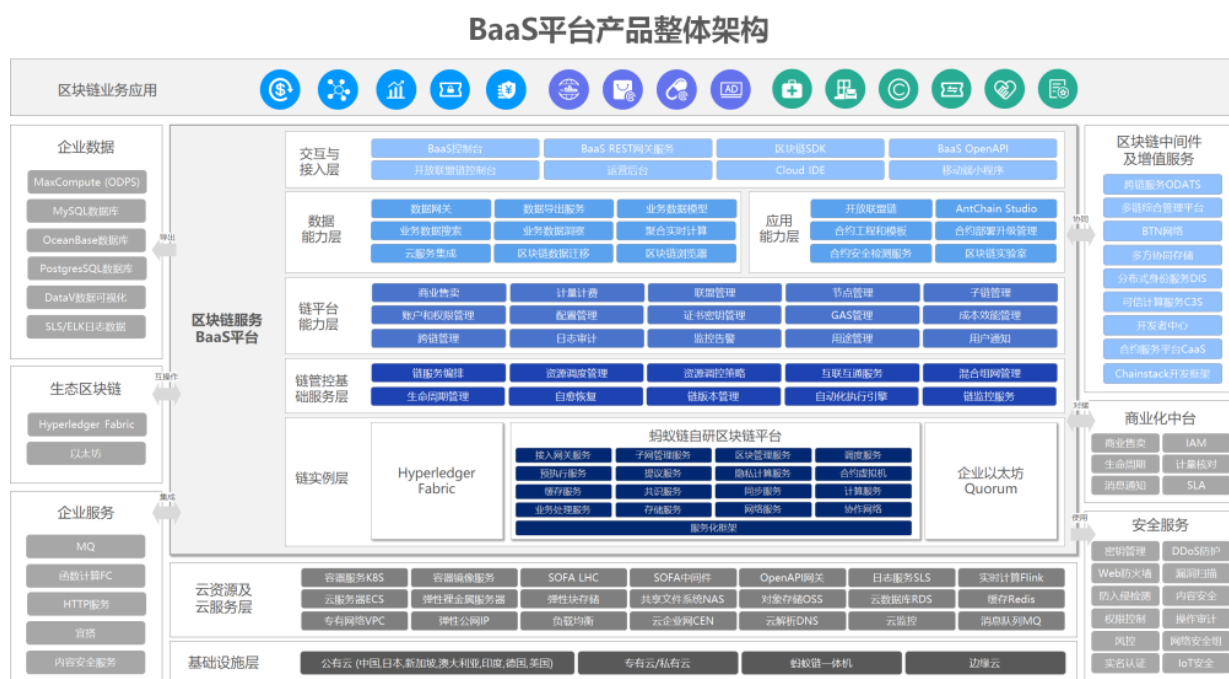
2. 产品架构

2.1 业务场景

企业和政务部门可以根据其数据安全和网络隔离需求，以私有化方式部署和搭建区块链服务网络，实现区块链管理、智能合约管理、应用连接管理，以及链上数据的导出与数据融合洞察、数字资产流转等功能。此外，平台还提供多种服务来提升数据价值，助力政企部门实现业务发展和数字化转型。平台还支持对区块链及相关服务的全方位监控与运维，实现全流程系统化输出。

2.2 产品核心架构

蚂蚁链 BaaS 平台产品核心架构如下图所示。



2.3 产品功能简介

2.3.1 BaaS 平台核心能力

BaaS 平台提供了区块链的搭建和管理、节点管理、证书及账户管理、智能合约工程管理、应用连接管理、运维中心、监控服务等主要核心能力。

2.3.2 BaaS 平台增值服务能力

BaaS 平台除了提供 BaaS 产品的主要核心能力外，为提供产品服务价值，支持在平台已有能力的基础上增加以下这些服务：

- **数据洞察能力**数据洞察包含数据导出服务和数据融合洞察服务的能力：

- 数据导出服务支持将区块链上特定的区块、交易、合约事件导出到外部的数据系统中，导出过程中保证事件的完整性，符合条件的事件会被推送到外部数据系统至少一次，便于用户对导出后的数据做进一步分析。
- 数据融合洞察服务支持链上精准数据及业务数据的搜索分析、链上数据关联打标、链上数据统计、链上链下数据融合展示、链上数据追踪及分析等能力。
- **跨链服务能力**跨链数据连接服务（ODATS, Open Data Access Trusted Service）以开源的 AntChain Bridge 跨链技术为核心，正逐步推进 IEEE P3205 互操作协议的落地，保证跨链交易的安全性、可扩展性及可靠性，打破区块链数据孤岛，实现同构及异构链之间的可信互通，助力企业之间可信协作，促进产业生态可信融合。除蚂蚁链本身支持跨链外，还支持七大异构链之间的跨链：fabric, bcos, 长安链，趣链，eos, eth, polygon。
- **一体化服务平台**一体化服务平台是一款专为加速产业数字化转型而设计的先进解决方案。该平台以其强大的技术整合能力、灵活的服务配置与卓越的兼容性，为企业提供了一个低门槛、高效率的区块链应用开发与管理环境。另外，平台主要聚焦于简化区块链技术的应用难度，赋能企业轻松构建安全、可靠且可扩展的业务应用，无缝融入各类产业场景。
- **多链综合管理平台**多链综合管理平台是一个具有异构链、异构 BaaS 纳管能力的统一聚合平台，为具有多种区块链引擎和厂商的用户提供了一致、便携的区块链平台管控能力。
- **多方协同存储**支持在多个协作节点组成的协作网络下创建并管理多个协作空间，并在协作空间内进行文件管理、空间下的账户管理的操作，所有操作均在链上留痕，便于追溯和审计。
- **区块链传输网络**区块链传输网络（Blockchain Transmission Network, BTN）是蚂蚁链为了解决区块链实际应用场景下的挑战而提出的网络优化解决方案。BTN 在区块链的 Layer0 层建立一个多链共享的区块链通信网络，提升区块链节点的网络稳定性、连通性、实时性的同时，解决联盟链成员变化彼此需要升级白名单等用户痛点。

3. 应用场景

3.1 政务场景

蚂蚁链基于 BaaS2.0 的 1+X+Y 架构全新发布了政务 GBaaS 平台，旨在从顶层设计为政府公共数据管理部门提供最佳实践参考，并通过国际标准认定跨链技术解决异构链接入成本高的问题，通过链上数据安全和共享平台解决数据跨链跨部共享难的问题，同时蚂蚁链在政务 GBaaS 平台提供了 oneID 和 oneData 等丰富的业务组件，帮助政府实现链上账户和身份的统一标识和管理。

3.2 供应链金融

蚂蚁链双链通以核心企业的应付账款为依托，以产业链上各参与方间的真实贸易为背景，让核心企业的信用可以在区块链上逐级流转，从而使更多在供应链上游的中小微企业获得平等高效的普惠金融服务。该产品已于今年 1 月份正式发布，并与一些核心企业在共同推进落地中。

3.3 溯源场景

利用蚂蚁链的技术能力，同时结合物联网技术，将商品从原材料采购，加工，生产，质检，物流，经销商，零售商一直到消费者手里全流程信息的可信记录，解决了信息孤岛，信息流转不畅，信息缺乏透明度等行业问题。目前天猫溯源应用比较广泛。

3.4 数字资产流向分析

企业在可信数据/数字资产的研发与运营中，这些资产在跨账户、跨链交易中的流向管理与透明度确保变得复杂而费时，数据融合洞察服务通过自动提取链上的数字资产及数据资产，利用强大的数据处理技术，将复杂的资产流动数据转化为直观、易懂的关系图表。桑基图汇总展示了某个账户资产的流动情况，以有色带的形式清晰标示出资产的来源及流向，直观地反映出资产流通的每一个环节。同时，该服务还结合了树图

和时间轴功能，提供了时间序列分析的视角，从而允许用户快速地追溯资产的流动历程，无论资产如何转移或跨平台交换，企业都能够精准追踪资产的每一步变化。

数据融合洞察服务提高了资产流转的可视化和透明度，让企业能够在资产流动的全过程中保持清晰的视线，这对于风险评估、财务审计、合规监管以及资产的战略决策至关重要。其次，简化了企业的资产追踪流程，节约了大量的人力和时间成本。在应对复杂的多链环境和快速变化的数字经济中，数据融合洞察服务确保了企业能够高效且精确地处理资产流动的监控与管理任务。通过数据融合洞察服务，企业不仅能够强化内部管理流程，也甚至能够在必要时向监管机构提供清晰、一致的数据报告，助力企业在新时代的数字资产管理中保持领先地位。

4. 产品功能

BaaS 平台提供全面的区块链基础管理功能，其核心能力具备区块链管理、证书管理、链账户管理、合约工程管理和监控运维等核心能力。此外，BaaS 平台支持部署多种提升区块链价值的服务，如链上内容审核、链上数据服务（数据导出和数据融合洞察）以及分布式协同存储。同时，平台还支持集成跨链数据连接服务（ODATS）和区块链传输网络（BTN），为用户提供强大的扩展性和灵活部署能力。

4.1 BaaS 平台核心能力

4.1.1 控制台功能

4.1.1.1 联盟链管理

BaaS 平台支持创建并管理多条区块链，每条区块链上可以部署多个节点，链类型支持标准合约链和国密合约链两种。在创建过程中，只需配置好链基本信息和节点信息后，即可自动化执行建链流程。

4.1.1.2 应用子链管理

BaaS 平台支持在区块链上创建子链，每条子链可以添加不同的机构成员和节点，为后续的业务隔离提供了方便，从而保证了数据的安全。支持查看子链上的区块链浏览器，并对子链上的链上账户、节点数、成员数进行管理。

4.1.1.3 跨子链授权管理

对于同一条链，其主链与子链之间或子链与子链之间可以进行跨子链授权。通过部署的业务合约调用系统级的跨子链服务合约（创建主链或子链时默认已部署好）来实现跨链数据访问。授权范围具体包含区块查询、区块头查询、交易查询、合约调用。在进行授权操作时，一次可以授权多种权限，并且后续也可修改它的授权范围，来灵活应对实时变化的业务需求。

4.1.1.4 证书管理

BaaS 平台已实现对区块链证书进行全生命周期管理的能力，满足用户在不同使用场景中对 BaaS 平台上与链建立 TLS 通信连接所需的访问证书的管理需求，具体包含以下管理能力：

- 创建并下载新的证书
- 删除已过期证书
- 冻结/解冻使用过程中的证书
- 下载签发证书所需的 CA 根证书

4.1.1.5 账户管理

与区块链进行交易时，除了需要获取与区块链建立 SSL 通信连接所需的证书、证书私钥及根证书文件外，还需要在目标链上创建一个区块链账户，从而通过账户维度在链上发起一笔交易。BaaS 平台支持在目标区块链（主链或子链）上创建多个区块链账户，

每创建成功一个账户，即可在账户列表下生成一条账户信息，同时获得链上账户的公私钥对及的恢复公私钥对。

4.1.1.6 节点管理

在管理主链的节点时，支持查看节点详情信息、添加节点（包括本地节点和域外节点），同时还可以操作节点的重启、停服/启服、节点配置信息的修改、以及节点共识状态的更新。

4.1.1.7 混合组网

通过添加域外节点的方式，将不同机房的节点部署在同一条区块链上，形成混合组网的区块链。混合组网的链支持通过全局管控视图和全局链视图，实时掌握链和节点的动态信息。当本管控配置了下级管理时，还支持通过为下级管控远程添加节点的操作，实现上下级管控上的链进行混合组网，方便上级管控对下级管控的管理。

4.1.1.8 智能合约管理

4.1.1.8.1 智能合约工程管理

用户可以根据业务情况选择使用空工程或合约工程模板创建合约工程。创建好的合约工程可以包含多个合约开发文件，同时与 Cloud IDE 结合使用，方便用户管理和开发智能合约。当合约部署到链上后，用户可在合约列表中对所有已部署合约进行管理，可根据业务情况操作合约冻结/解冻。

4.1.1.8.2 智能合约工程模板

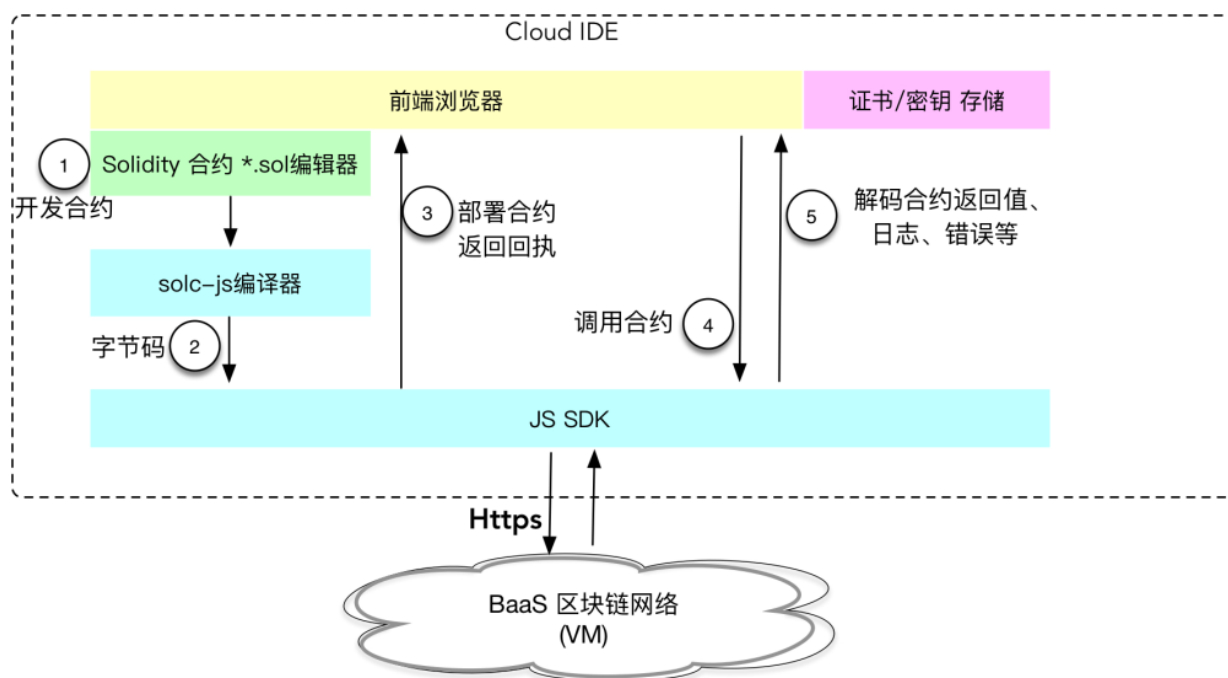
很多存证类合约的很多功能都有固定的格式代码对应，例如增、删、改、查功能、权限控制功能、日志功能、时间触发器等。因此，蚂蚁链提供一套自动化的智能合约代码生成工具，帮助用户通过配置数据表的形式来快速定义和生成合约，提高效率。

4.1.1.8.3 智能合约开发工具

在区块链应用开发过程中，需要调用您的智能合约，智能合约主要用于调用区块链。为提高基于蚂蚁链的开发效率，BaaS 平台提供了 Cloud IDE 智能合约开发工具和 AntChain Studio 本地智能合约开发工具，帮助您快速实现智能合约的开发。

Cloud IDE

Cloud IDE 合约开发环境（以下简称“IDE”）是 BaaS 合约平台提供的在线合约开发工具。IDE 是一个典型的去中心化应用（Dapp），可通过 JavaScript SDK 直接与区块链平台通信，进行合约部署和调用。这样设计的优势在于，通过 IDE 您可以连接任何目标的蚂蚁区块链平台环境。



IDE 为智能合约开发提供简单、高效的集成环境，并提供以下核心功能：

- 合约工程管理：管理工程目录和文件，提供文件编辑自动保存功能，保存合约到 BaaS 合约管理。
- 合约编辑与编译：展示编译结果字节码和接口说明（ABI）。
- 合约的部署和调用：提供默认合约体验链环境和测试账户，用来部署和调用合约。

- **自动编解码**：解析合约方法的返回值、事件日志等，辅助合约测试。
- **合约单步调试**：当前支持 Solidity 合约的单步调试功能，可单步执行，查看临时变量、合约存储、堆栈、内存等信息来深度调试合约。
- **合约单元测试**：当前支持 Solidity 合约的单元测试，可直接使用 Solidity 语言编写单元测试用例，一键执行所有测试用例。
- **合约分析**：在编译合约的同时对 Solidity 合约进行静态扫描分析，给出分析结果参考。

AntChain Studio

AntChain Studio 是一款面向区块链智能合约研发，易用低门槛、多语言、快速研发、一体化集成的本地智能合约 IDE，让 DApp 开发更快更友好更专业。

AntChain Studio 致力于服务蚂蚁链生态应用研发，打造一站式集成开发环境，内含多种合约语言，覆盖合约开发的整个生命周期，集成蚂蚁链中间件，支持基于框架开发与专业合约开发：应用代码生成、一键编译部署、可视化合约测试等，为用户提供具备低门槛、简单易用、快速研发的智能合约研发框架，方便用户高效上手区块链应用研发。

AntChain Studio 特点

- **快速智能合约研发**配套**专业智能合约研发课程**与**可视化合约操作**界面，**无需任何一行代码**，新手用户也能快速接入**区块链网络**，一键创建智能合约工程、部署上链并可**可视化调试**，实现用户快速研发、部署、调试智能合约。
- **一站式集成开发环境**一体化集成蚂蚁链区块链研发工具，涵盖 MYCDT 编译工具与 ChainStack 企业级研发框架，提供具备**低门槛、简单易用、快速研发**的智能合约研发框架以及配套多种解决方案的**区块链应用原型**，支持业务快速搭建 DAPP 应用。
- 一套企业级研发工具依托蚂蚁链平台开放行业领先的金融科技区块链服务，提供开发环境**自动配置**、应用/合约代码**自动生成**、**多语言**合约编写，**一键编译部署**，快

速调试的智能合约开发服务，覆盖 DApp 应用的整个生命周期，加速用户智能开发、测试。

- 可视化调试区别于传统智能合约研发方式，AntChain Studio 为用户提供**可视化调试界面**，只需要选择想要调试的合约接口并填写测试数据，即可**自动保存测试用例**、一键运行并展示测试结果。
- 一套高效友好开发框架一套专门为区块链应用 dapp 打造的高效友好研发框架，涵盖**智能合约框架与类库**、dapp 后端应用框架、spring 集成、**应用原型**等，适用于企业级区块链应用平台研发。

核心功能



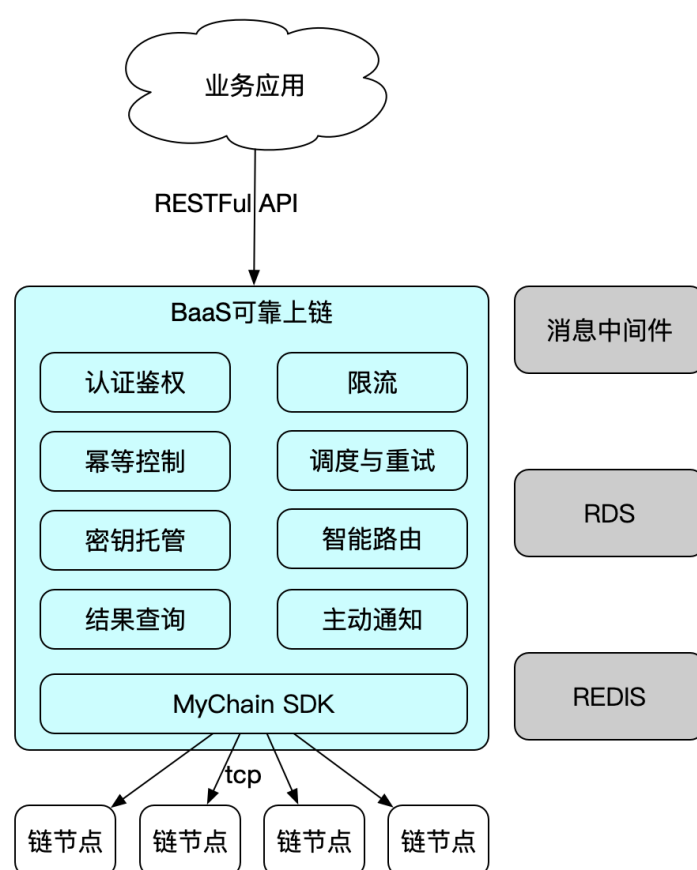
4.1.1.9 区块链浏览器

区块链浏览器展示了丰富的节点实时运行指标，包括链交易数目、节点信息、账户信息、出块信息、块中包含的交易等信息。同时，平台还支持免登录方式进入目标链的区块链浏览器中查看链交易相关的数据。

4.1.1.10 REST 网关管理

REST 是蚂蚁链 BaaS 平台官方提供的接入服务，目标是为上层区块链应用提供易用、高效、可靠的统一区块链接入服务。

REST 提供合约管理、账户管理、合约交易、存证交易、区块查询等蚂蚁链常用交互功能，以及 MYTF 链下安全计算应用管理和应用执行操作功能，同时集成和利用蚂蚁生态中的区块链基础服务设施和核心技术能力，包括 KMS 和 TEE，提供多种灵活的区块链访问方式，同步/异步调用，外部/内部签名，普通/私密交易。以下是 BaaS REST 可靠上链的完整的功能示意图。



4.1.1.11 运维管理

在运维管理方面，提供的审计日志可以记录操作链管理、合约管理、链接管理、数据导出服务、跨链服务等的所有事项，方便机构成员及管理者的日常审计。另外，平台

还提供运维记录的执行和查看操作，如涉及建链、节点管理等相关操作时，均可通过运维记录跟踪节点安装，配置，进程等信息。

4.1.1.12 监控中心

BaaS 平台接入了 Watchman 监控组件，旨在为 BaaS 平台提供区块链指标数据的背景下，基于时间序列数据库基础上，以通用适配的模式接收各大类区块链的采集的指标数据及日志信息，实现指标的统一处理，提供指标的聚合查询、资源查询、日志查询、告警通知等功能。

4.1.1.12.1 监控服务

监控服务模块提供了链监控和服务监控两种监控对象，相关功能描述如下：

- **链监控**基于 BaaS 平台，提供多维度链节点监控指标，具体包括共识、交易、区块、链存储、磁盘、系统、内存、CPU、网络维度的监控指标。通过这些监控指标，可以实时反应链的运行情况以及主机资源的占用情况，帮助用户合理规划链的使用。
- **服务监控**基于 BaaS 平台，提供多维度服务监控指标，具体包括全局维度、链维度、接口维度、业务维度、磁盘、系统、内存、CPU、网络维度的监控指标。通过这些维度下提供的监控指标，可以实时监控该应用服务的运行情况以及资源占用情况，帮助用户合理规划内存资源和应用服务的进程数。

4.1.1.12.2 告警管理

告警管理模块支持用户针对目标链节点自定义选择链监控指标，通过对这些指标设置阈值，来触发告警。其中告警通知方式可以选择钉钉机器人或邮箱通知，并在可配置的告警策略下完成告警通知。通过告警规则的设置和告警记录的查看，用户可以及时掌握链上异常状态并做出响应。

4.1.1.12.3 服务日志

链在运行过程中会产生大量日志信息，大部分日志专业性比较强，通常需要具备专业知识的技术人员来解析。监控中心提供的服务日志提供了强大的筛选功能，支持用户

筛选出目标链节点从起点时间之后的节点日志或合约日志，帮助用户优化合约、排查问题，从而提升应用性能。同时，筛选出的日志信息，支持实现快速查找与便捷复制的功能。

4.1.2 区块链开发

4.1.2.1 什么是区块链应用

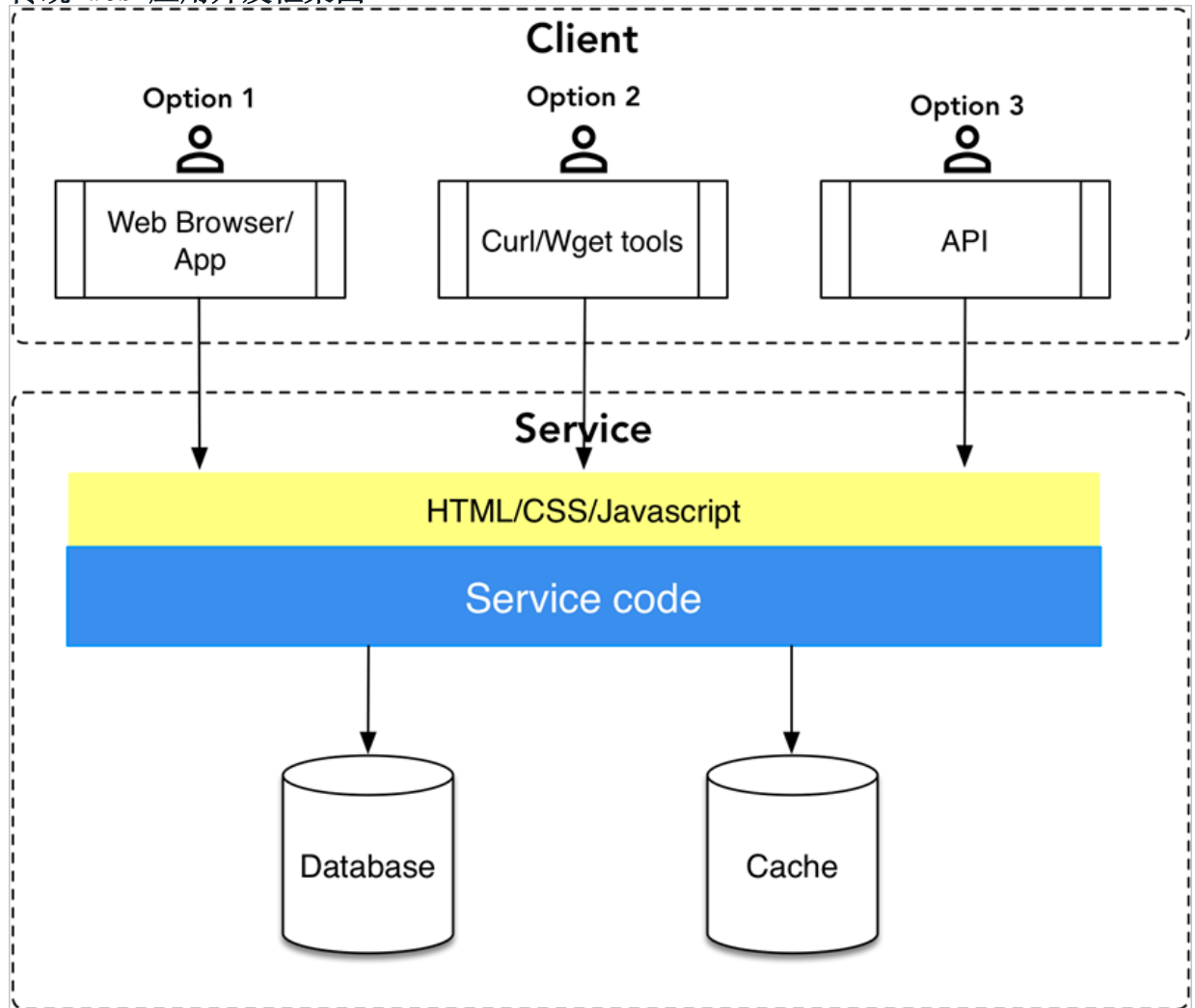
区块链应用 DApp (Decentralized Application) 就是去中心化应用。DAPP 就是基于 P2P 对等网络而运行在智能合约之上的分布式应用程序，区块链则为其提供可信的数据记录。

4.1.2.2 与传统应用的区别

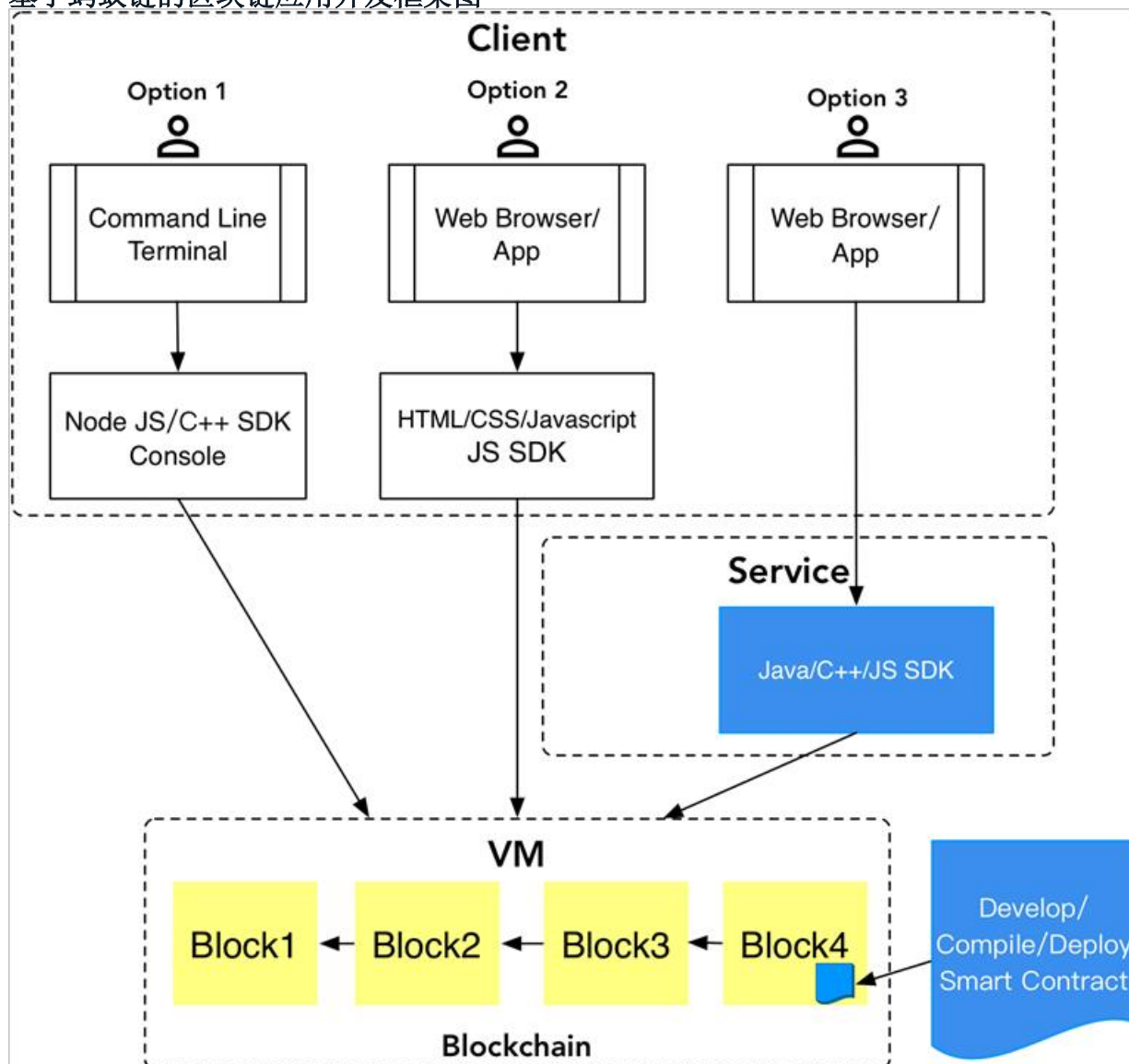
传统的 Web 应用开发通常由客户端和后端服务组成。而基于蚂蚁链的区块链应用开发除了客户端和服务端开发，还需要开发区块链上运行的智能合约。

简单来说，区块链应用是通过调用智能合约将数据存储区块链的传统分布式应用，或通过直接调用的方式将数据存储区块链的传统分布式应用（没有使用合约的场景）。所以 DApp 和传统 APP 的区别从技术的角度看，区别在于 DApp 的数据是存储在区块链上的，确保难以篡改；而传统 APP 的数据是存储在传统数据库上，可以直接修改。

- 传统 Web 应用开发框架图



- 基于蚂蚁链的区块链应用开发框架图



4.1.2.3 区块链应用开发方式

基于蚂蚁链的区块链应用开发时，您可以有以下 2 种链接入的方式：

- 方式 1：通过 SDK 与蚂蚁链进行交互，包括账户服务、查询服务、合约服务、查询服务等等操作。
- 方式 2：通过 REST 与蚂蚁链进行交互，包括合约管理、账户管理、合约交易、存证交易、区块查询等蚂蚁链常用交互功能，以及 MYTF 链下安全计算应用管理和应用执行操作功能。

应用开发场景主要有以下 2 种方式，您可以根据具体应用场景进行选择：

- 选项 1：通过 Web 应用（Client）集成 SDK 或 REST 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 2：与传统 Web 应用开发相似，访问后端服务（Service），后端服务集成 SDK 或 REST 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，在后端服务层实现一些比较重要的业务逻辑和计算任务。

4.1.2.3.1 多语言区块链 SDK

为适应不同的客户群体，蚂蚁链提供多语言 SDK 支持，包括：

SDK 语言	功能特性	说明
Java	功能最丰富，覆盖蚂蚁区块链所有的功能。	适合用于后端服务层。
C++	功能丰富，与 Java SDK 功能相似。	比较适合与传统 C++ 服务相结合。
Java Script	覆盖基本常用的 API，支持 Node.js 和浏览器环境运行，不支持国密。	适合客户端 Web 应用集成。

4.1.2.3.2 RESTful 接入

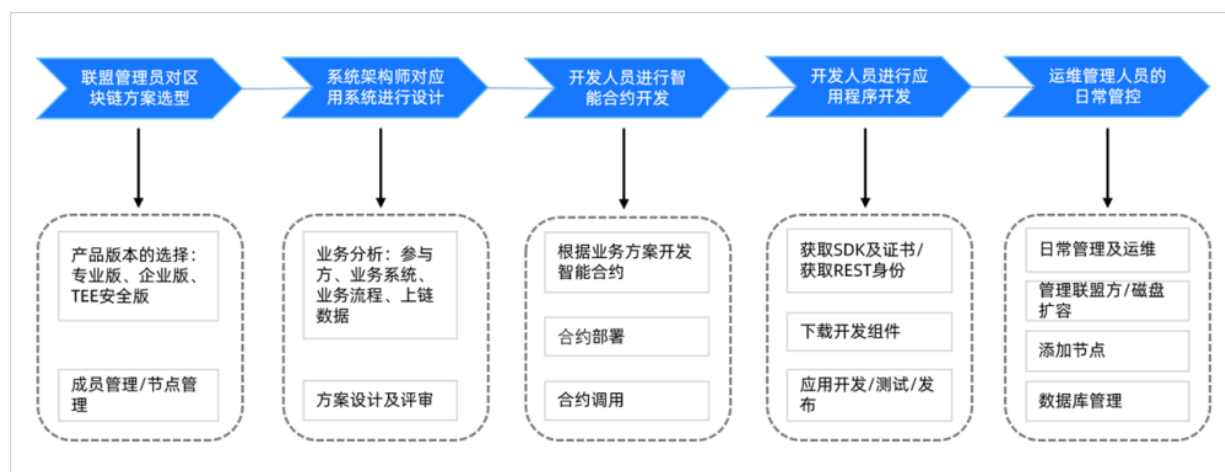
REST 接入服务的具体优势如下：

- 标准化接口：跨编程语言标准的 RESTful API 接口。
- 灵活性编程：支持同步调用、异步调用、主动轮询、异步消息、托管代签等模式。
- 可靠性服务：幂等控制、可靠上链、可靠推送、异常重试、交易数据持久化，智能路由能够选择最优节点来发起上链交易。

- 稳定性保障：限流降级、细粒度监控告警。
- 安全性护航：AK/SK 及访问令牌、TEE 链加密交易
- 高性能支撑：结合数据分片、水平扩容、交易缓冲等技术，具备日均 10 亿规模交易处理能力。

4.1.2.4 区块链应用开发流程

在使用蚂蚁链进行区块链应用开发过程中，您需要开发自己的智能合约和应用。在实际业务实现中，基于蚂蚁链的区块链应用开发并不约束于具体的开发流程，以下只针对业务层面展开的流程介绍。



说明：智能合约开发并不是区块链应用开发的必要环节，您需要根据实际业务场景选择是否进行智能合约的开发。

4.1.3 智能合约开发

4.1.3.1 智能合约语言

智能合约（Smart Contract），是一种旨在以信息化方式传播、验证或执行合同的计算机协议。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。



目前，蚂蚁链支持 Solidity、C++、Golang、TypeScript 及 Java 五种语言，基本涵盖了所有流行的合约编程语言。

4.1.3.2 智能合约平台

蚂蚁链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，从而实现丰富的业务场景。

- 合约生命周期蚂蚁链中，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、合约冻结六个环节。



- 合约类型蚂蚁链提供图灵完备的智能合约能力，目前提供 WASM 和 EVM 两种合约类型。其中，WASM 合约类型支持多种常见通用编程语言开发合约（如 C++、Java、Go、AssemblyScript），并通过 JIT 即时编译技术提供高性能的合约执行性能，EVM 合约类型支持 Solidity 合约编程语言。
- 合约扩展蚂蚁链智能合约提供了多种形式的合约扩展能力，包括 RSA 验签、Base64 编解码、上下文获取、JSON & XML 解析等。

4.1.3.3 智能合约审计

蚂蚁链从静态分析，模糊测试，形式化验证三个技术方向提供全面的合约安全保障。静态分析工具具备 100 多条检测项，覆盖 250 多种业务场景，提供包括编码规范、执行效率优化，编译器版本 bug，常见安全漏洞在内的多种检测能力；模糊测试工具深度结合合约开发框架，提出自生成模糊测试用例方法，保证最终代码行覆盖率达到 90% 以上，可显著发现边界安全问题；形式化验证工具，通过友好的前端安全规范语言降低使用门槛，使一般开发者能够在 15 分钟内学会使用该工具。同时结合了符号执行技术和抽象理解技术来解决形式化验证技术普遍遇到的状态空间爆炸问题，支持对上万

行代码的超复杂合约进行验证。通过在大量真实合约上持续运行的积累，根据公开信息比较，蚂蚁链安全审计工具在执行效率，检出率和误报率上均处于行业领先水平。

4.1.4 链底层能力

4.1.4.1 共识算法

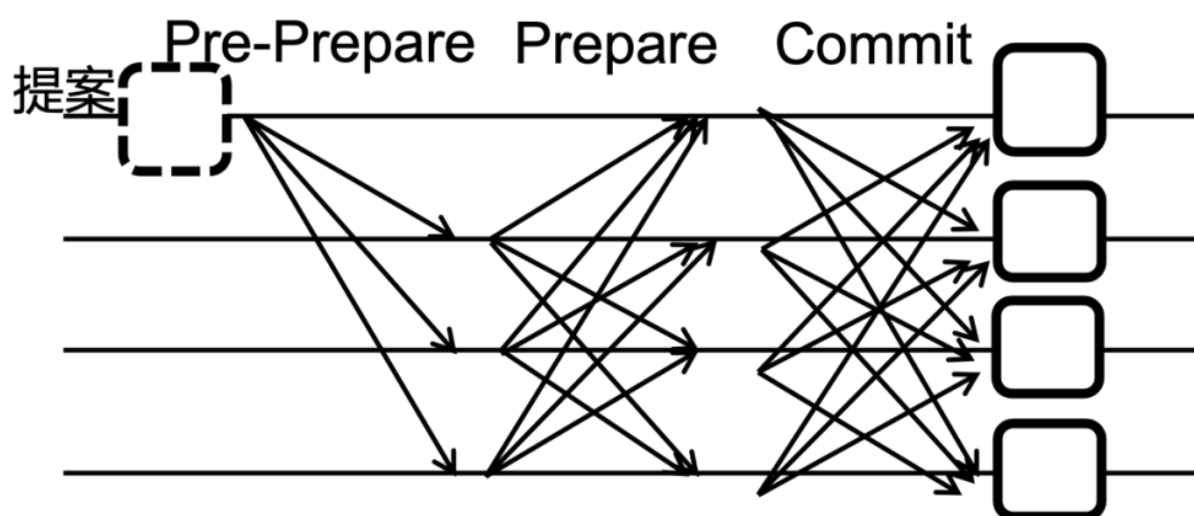
在蚂蚁链中，共识协议被定义为使分布式系统中的节点快速有效地达成数据一致性的协议，即确保所有诚实节点以完全相同的顺序执行共识结论中交易，达成数据一致性，同时正确的客户端发送的有效交易请求最终会被处理和应答。

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

4.1.4.1.1 PBFT 共识算法

PBFT(Practical Byzantine Fault Tolerance)是一种在半同步网络下运行的有主共识协议，能容忍系统中存在不超过 $1/3$ 的拜占庭节点。为了简化说明，假设系统中共有 $n=3f+1$ 个共识节点，其中 f 是拜占庭节点的数量。

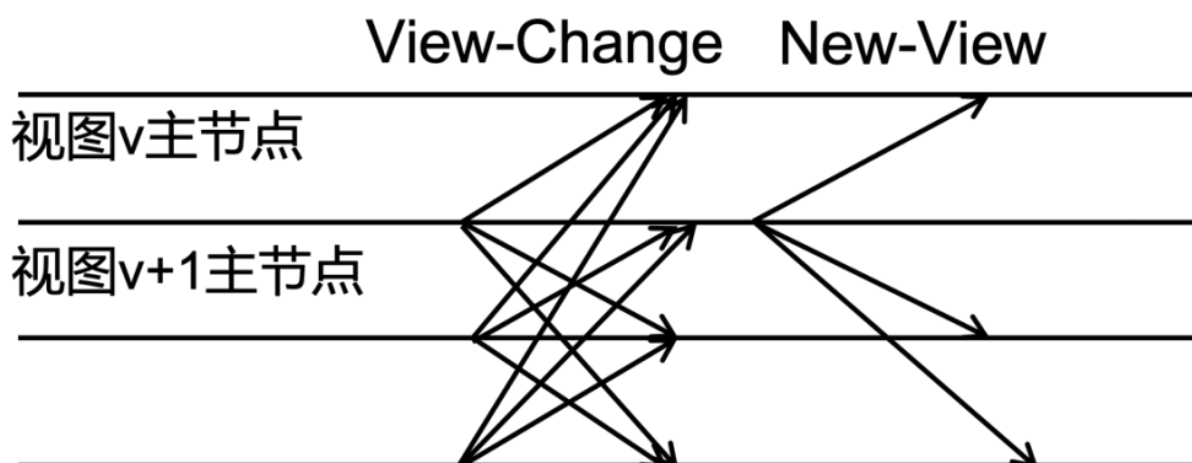
具体而言，PBFT 正常流程包括三个阶段，如下图所示：



- Pre-Prepare 阶段：主节点将一批交易打包成一个提案广播给所有从节点；

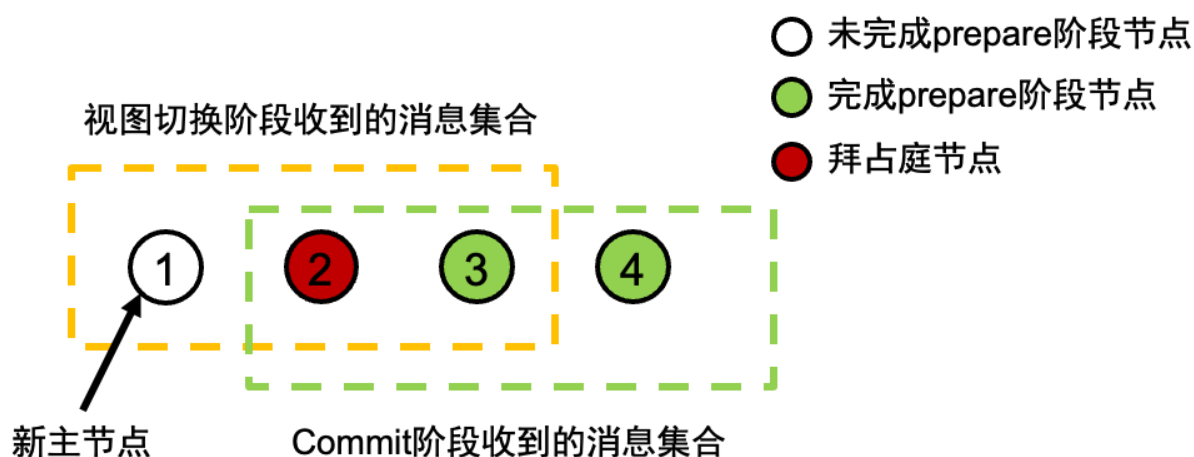
- Prepare 阶段：从节点收到主节点的 Pre-Prepare 消息后，若验证通过则广播 Prepare 消息，表示自己对该提案的认可（第一轮投票）；
- Commit 阶段：共识节点收到 $2f+1$ 个来自不同节点对同一提案的 Prepare 投票后，广播 Commit 消息（第二轮投票）；当收到 $2f+1$ 个来自不同节点对同一提案的 Commit 投票时，可以确认该提案是本轮共识最终产生的区块。协议的安全性保证了所有共识节点在该区块高度最终都将提交同一区块。

PBFT 协议按照视图（view）来运行，每个视图对应一个确定的主节点，当主节点是拜占庭节点或网络波动因而未能及时完成共识时，从节点会发起视图切换子协议来更换主节点，如下图所示：



- View-Change 阶段：从节点本地超时触发后，广播 View-Change 消息，要求更换主节点，View-Change 消息内携带了该节点当前共识的进度；
- New-View 阶段：新的主节点收到 $2f+1$ 个来自不同节点的有效 View-Change 消息后，根据这些节点当前的共识进度，计算出在保证一致性的前提下如何继续进行共识，并将计算结果放入 New-View 消息广播给所有节点，同时携带上述收到的 $2f+1$ 条 View-Change 消息来证明 New-View 消息的合法性。

视图切换子协议保证了即使不同节点当前共识进度暂时不一致，在视图切换后不会破坏最终共识的一致性，如下图所示：



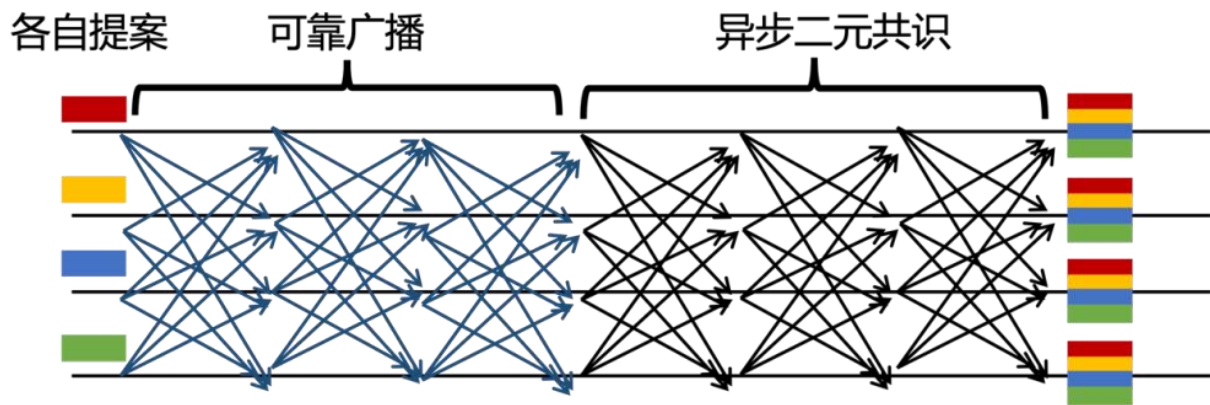
绿色方框表示某个节点已经收到了足够多 ($2f+1$) 的 Commit 消息并提交了该轮共识的结果, 此时其他节点可能尚未收到足够多的 Commit 消息并发生了视图切换, 而新的主节点收到的 $2f+1$ 条 View-Change 消息内一定会包含某个诚实节点 (节点 3) 参与了上述 Commit 阶段, 在得知存在节点已经对某提案进入 Commit 阶段后, 该新主节点必须对该提案重新进行共识, 最终所有节点在这一区块高度仍然会提交相同的共识结果。

蚂蚁链实现的 PBFT 共识协议不仅能够容忍不超过 $1/3$ 的拜占庭错误, 还通过关键消息和状态的持久化保证了任意数量的诚实节点宕机重启后的状态一致性, 相比于原始算法提供了更强的鲁棒性。此外, 蚂蚁链提供的 PBFT 共识插件支持使用交易哈希进行共识, 即主节点的提案内仅包含交易的哈希而非交易原文, 从而降低主节点的网络带宽消耗, 提升共识效率。

4.1.4.1.2 ABFT 共识算法

ABFT (Asynchronous Byzantine Fault Tolerance) 是一种在异步网络下运行的无主共识协议, 同样能容忍系统中不超过 $1/3$ 的拜占庭节点以及保证任意数量的诚实节点宕机重启后的状态一致性。相比于 PBFT, ABFT 无需依赖单一主节点进行提案, 实现了共识节点间角色的完全平等; 同时由于 ABFT 基于纯异步网络的假设而设计, 因而不需借助超时机制, 可以在网络情况不稳定、延时较高时健壮地运行。

具体而言, ABFT 包含两个子过程, 分别是可靠广播和异步二元共识:



- 可靠广播 (Reliable Broadcast, RBC)：系统中某个发送节点广播一条消息，经过 RBC 协议最终所有诚实节点或全部输出这条消息，或全部没有输出。RBC 协议保证了节点间的一致性，但并不提供活性，即若发送节点是拜占庭节点，所有诚实节点可能全部卡住无法产生输出；
- 异步二元共识 (Asynchronous Binary Agreement, ABA)：对于某一提案，所有共识节点的初始输入为 0 或 1，经过 ABA 协议最终所有诚实节点或全部输出 1 或全部输出 0，若共识结果为 1 表示该提案最终可以上链，若共识结果为 0 表示该提案无法上链。ABA 协议保证了若所有诚实节点初始输入一致，则最终输出也一定是这一输入。

在 ABFT 协议中，对于每一区块高度，所有共识节点将各自提案，即作为发送节点发起自己提案的 RBC 协议。每个提案将对应到一个 RBC 实例和一个 ABA 实例。若某个 RBC 实例完成，即输出了其对应的提案，节点将向该提案对应的 ABA 实例输入 1；当 $2f+1$ 个 ABA 实例最终输出了 1，节点将向剩下尚未完成 RBC 的提案对应的 ABA 实例输入 0。最终 n 个 ABA 实例都将输出 1 或 0，将其中输出为 1 的实例对应的提案按照确定性顺序组合就构成了该区块高度最终共识的结果。

4.1.4.1.3 PBFT 和 ABFT 共识算法特性对比

共识算法	优点	缺点	建议使用场景
PBFT	• 1/3 拜占庭节点容错，任意数量宕机恢复容错	• 依赖单一主节点提案，节点带宽使用不	4-100 共识节点，网络环境稳

(默认)	正常无错情况下延迟低，三轮消息交互完成共识	均衡 主节点异常将触发超时换主流程，会造成短暂性能波动	定，高性能场景
ABFT	1/3 拜占庭节点容错，任意数量宕机恢复容错 - 节点身份对等，不依赖单一主节点，充分利用带宽 - 不依赖网络延迟假设，在网络不稳定时具有强鲁棒性	消息交互轮数高于 PBFT，因此延迟也相应较高	100 以上共识节点，公网大规模集群，尤其是广域网、高带宽、高延迟或不稳定的网络

4.1.4.2 加密算法

密码学是区块链信任的安全基石，蚂蚁链平台即是通过密码学套件和协议实现了区块数据的不可篡改、可追溯、共识和交易的不可否认等特性，从功能上看，密码学在蚂蚁链中主要功能如下：

- 区块数据的一致性以及不可篡改、可追溯能力**蚂蚁链是采用了杂凑算法实现的哈希链，通过区块哈希来锚定区块数据，确保数据无法被篡改，同时以哈希链条的方式实现了数据可追溯能力；结合标准非对称算法的 PKI 体系和共识机制，保证了区块链数据的一致性；
- 交易授权、鉴权和身份认证能力**蚂蚁链采用了非对称算法进行签名验签，实现交易授权、鉴权和身份认证，链上节点、用户、管理员均需通过在链上注册过的密钥对完成交易、请求、消息等内容的签名，验证时由节点根据发送方信息检索链上保存的密钥对信息完成签名验证，确保了交易、消息等内容的完整以及不可篡改和伪造；

- **安全通信传输能力**蚂蚁链的数据通信均采用了 TLS 加密通信机制，提升了客户端交互以及链节点交互的数据安全性。其中，蚂蚁链采用了基于 RFC8998 的 TLS1.3 国密套件，并对所有较弱套件做了筛选，具有较高的安全防护能力。

针对上述功能中涉及的算法支持方面，蚂蚁链平台具有完整、安全以及高性能的国际/国密的版本实现。

国密算法与国际标准算法主要区别体现在自主安全性、自主可控和合规性。SM 系列国密算法完全满足国家政府部门安全要求，是国家信息安全的基础设施；且完全由我国科研人员自主设计，符合自主可控的标准。

蚂蚁链为了满足对于国密合规等密码安全需求，蚂蚁链平台提供了软件和硬件两种密码模块的解决方案，其中国密软件模块采用了具备国密资质的 SHM1933Linux 软件密码模块，硬件密码模块采用了具备国密三级资质（目前商密产品中的最高级别）SJK19150 的密码卡。因此，蚂蚁国密链和非国密链的区别仅在于上述密码学算法的实现标准上，而在蚂蚁链的数据交互、交易执行、数据处理、技术拓展等方面并没有区别，目前蚂蚁链支持的主要密码学算法实现标准如下：

算法		种类	类型
数字签名	Secp256k1（默认）	ECDSA	国际
	Secp256r1	ECDSA	国际
	SM2	SM2DSA	国密
	RSA2048	RSA	国际
非对称加解密	Secp256k1（默认）	ECIES	国际
	Secp256r1	ECIES	国际
	SM2	SM2IES	国密

	RSA2048	RSA	国际
杂凑算法	SHA256 （默认）	杂凑算法	国际
	Keccak256	杂凑算法	国际
	SM3	杂凑算法	国密

4.1.4.3 并行调度引擎

调度引擎是协调本区块链中的核心数据结构，即区块和交易的流转。具体来说就是区块什么时候进入共识阶段，或者执行阶段，以及交易什么时候进入执行阶段等等。这里的并行调度指的是两个维度的并行：

- 区块间执行步骤的并行，即不同区块下的共识和执行可以同时进行。
- 区块内交易的并行执行，即同一个区块内的不同交易按照一定的依据可以同时执行。

4.1.4.4 智能合约虚拟机

克服了垃圾回收，虚函数，异常处理，反射，注解等众多技术难点，最终所有语言均实现在 EVM3.6.1 或者 WASM3.6.2 虚拟机环境当中，相较于容器(Docker3.6.3)环境和 JVM3.6.4 环境能够提供更高的安全级别，实现安全性与功能性的有机结合。

- **高性能 JIT 编译技术**解释执行性能低，而 Native 二进制程序虽然执行效率高，但直接部署二进制代码面临“二进制被篡改”的安全风险，导致虚拟机安全沙箱限制被突破。蚂蚁链结合实际场景中的安全与性能需求，自研 JIT 编译器。经实测，蚂蚁链智能合约 JIT 引擎在 DES，MD5，RegEx，SHA256 等计算密集型任务上，相比较开源虚拟机 WAMR 解释执行模式，分别达到 26.5 倍，21.7 倍，28.5 倍及 24.1 倍的加速效果。其应用于常见业务合约上，实现了整体平台端到端 TPS 的 2 至 4 倍性能提升。同时，蚂蚁链智能合约 JIT 引擎不依赖任何系统调用，可完美兼容现有可信执行环境产品，如 Intel SGX，国产 TEE 及蚂蚁链自研 TEE。根据公开信息，区块链社区常用的 JIT 引擎都不支持此特性。

- **四层合约数据处理能力**蚂蚁链提供多种数据处理语言，同时支持 KV 和 SQL 两种不同的合约数据模型。在保证区块链数据可验证特性的前提下，实现了从用户自定义数据以及结构化数据到底层存储数据的映射，实现了合约数据定义，访问，遍历，以及查询的四层处理能力。根据公开信息，社区常用的编程语言，如 Solidity，通常仅支持 KV 模型，只提供数据定义和访问两层能力。

4.1.4.5 隐私保护

- **零知识证明**设计了关于 Paillier 公钥合法性与密文正确性的零知识证明协议，提升安全多方计算安全性，实现基于半同态加密算法的恶意安全模型。提供了通用零知识证明编程框架，实现合约级的可验证隐私保护，提供范围证明、集合关系证明、非集合关系证明、所有权证明、计算过程证明等功能。
- **分布式签名算法**针对椭圆曲线签名算法，特别是国密 SM2 算法，提出了改进型算法，在传统算法基础上支持任意门限值、支持动态门限变更、动态私钥分片轮转，同时相比传统多方签名技术，降低交互轮次，提升交互效率。
- **匿名签名**匿名签名技术在区块链账户身份的隐私保护中有着广泛应用，主流方案使用环签名技术。蚂蚁链提出了理论最优的环签名和门限环签名算法，尺寸分别为业界的 $4/5$ 和 $1/2$ 。同时引入可监管陷门技术，实现联盟链关键业务的有效、安全的合规治理。
- **隐私保护算法**基于全同态的联合建模较业界计算性能提升 $1\sim 2$ 倍。基于 SQL 语义的匿踪查询算法，支持亿级数据规模下、百万混淆集安全性下的秒级查询能力。基于 VOLE3.3.4, 3.3.5 的大规模乘法三元组构建协议，大大提升 MPC 计算效率，比业界综合开销降低 95%。

4.1.4.6 存储

4.1.4.6.1 存储服务

蚂蚁链自研了分布式存储服务 MyGrid，支持存储计算分离、区块数据范围分片、集群弹性可伸缩、存储引擎可插拔、元数据高可用等，为区块链平台提供高性能低延迟的数据存储服务。

- **存储计算分离** MyGrid 采用了分布式存储架构，支持单个共识参与方计算和存储分离。蚂蚁链的计算层和存储层可分别部署独立集群。计算集群的服务进程，通过存储服务 SDK 接入存储集群，依托高性能网络通讯框架 ERPC 进行数据读写访问。
- **区块数据范围分片** MyGrid 支持区块数据的范围分片，并支持多种存储引擎灵活混合使用。比如第 1 块到第 N 块使用 RocksDB 存储，第 N+1 块到第 M 块使用 LETUS 存储等。
- **集群弹性可伸缩** 存储集群支持弹性扩缩容，可根据业务需要对集群进行扩容或者缩容。例如在系统初始化的时候，使用 2 个物理机器来构建一个存储集群，后来随着业务的发展，数据量越来越大，TPS 越来越高，可以选择在存储集群里增加两台物理机器，提供更高的带宽和吞吐。如果过了一段时间，业务量有所下降，对带宽和吞吐要求降低，则可以把集群缩容至两台机器，来降低成本。
- **存储引擎可插拔** MyGrid 支持多种存储引擎，可以选择 RocksDB、LevelDB 等开源数据库，也可以选择蚂蚁链自研存储引擎 LETUS。同时，用户也可以自行实现一套 MyGrid 定义的标准接口，把第三方的引擎接入 MyGrid。
- **元数据高可用** MyGrid 采用 etcd 进行元数据管理，依托 etcd 自身的高可用特性，实现了 MyGrid 元数据高可用。

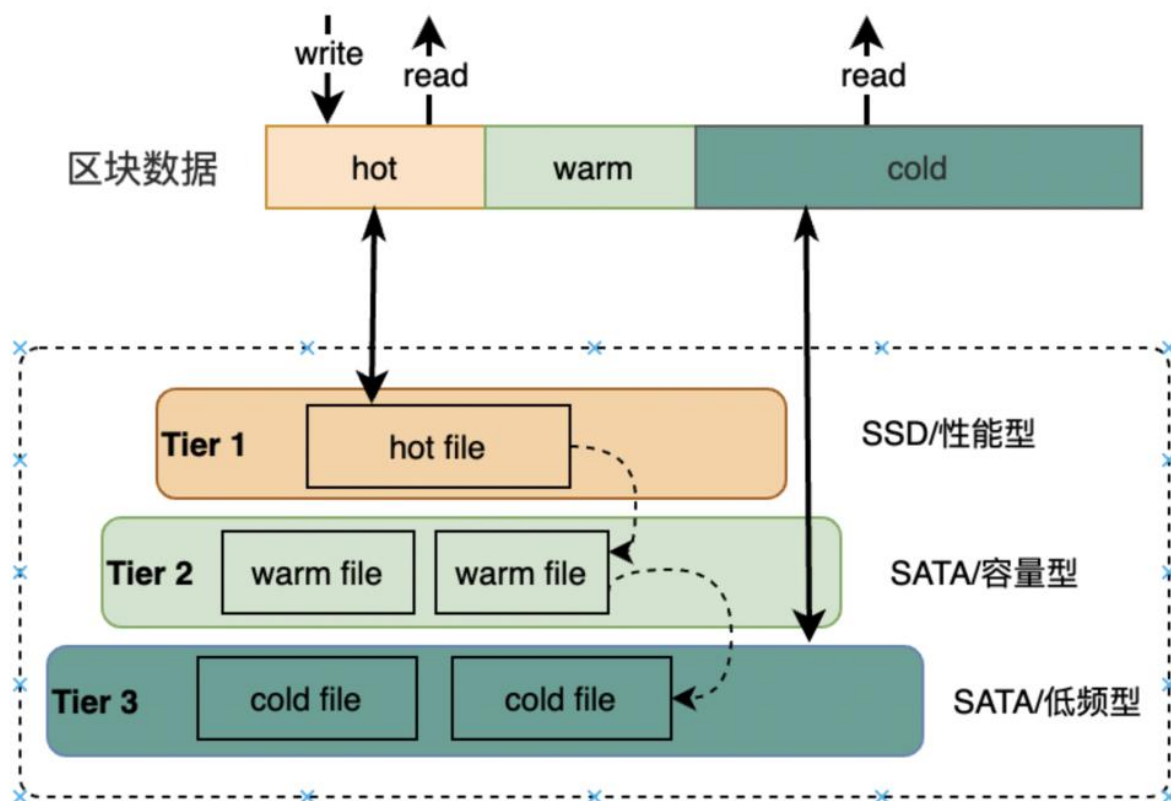
4.1.4.6.2 存储引擎

蚂蚁链自研的存储引擎 LETUS，充分利用账本追加特点，基于 Log-structured 架构实现日志即数据，通过多模扩展的非聚簇索引和可拓展数据治理框架，支持灵活的

GC/Tiering/Verification 等后台数据治理功能，从而为区块链平台提供了大规模、高性能、低成本的链上数据管理。蚂蚁链自研存储引擎 LETUS 主要具备以下几个特点：

- **大规模和高性能支持**蚂蚁链自研存储引擎支持海量账户资产，在区块存储效率方面，相较于业界普遍使用 RocksDB/LevelDB 存储引擎，LETUS 引擎的区块数据访问的磁盘带宽占用下降约 50%，性能也远高于传统区块链存储。
- **极大的降低区块链节点成本**
 - **支持区块链数据归档**蚂蚁链支持区块数据自定义归档能力，用户可通过数据归档工具，对历史区块体（交易和收据）数据进行归档，仅保留历史区块头、降低历史数据的成本压力，提供基本的区块校验和 SPV 能力。
 - **支持区块链数据的冷热迁移**针对区块数据，考虑到历史区块的低频访问特性，可实现热点区块数据保存在高性能存储介质中，满足业务读取以及节点数据同步的高频需求，而历史区块保存在廉价介质中降低成本，同时提供可靠访问能力。蚂蚁链已实现区块数据根据规则自动迁移冷热数据，可降低约 70% 的存储

成本，并降低运维成本。



- 支持数据可验证、快速多版本查询等多种能力

4.1.4.6.3 开放存储

蚂蚁链开放存储提供了一套以结构化的形式直接访问链上数据的解决方案。蚂蚁链开放存储支持链上区块数据实时写入结构化数据库，并提供一定的预处理能力。用户可通过 SQL 查询进行大规模数据查询和分析，并可以根据自身对链上数据访问的业务应用模式实际需求，选择使用不同的数据存储引擎。

为了便于业务合约能更高效便捷地接入到结构化系统中，蚂蚁链开放存储定义了一套针对合约方法、参数以及回执输出内容的通用框架规则。合约通过制定一套统一的弱格式 Schema，实现对业务输出字段的自适应解析。针对不同的应用场景，合约业务解析框架拥有足够的灵活度及完备的可扩展性，通过将链上区块数据预处理放到结构化数据库，为业务实现链下复杂查询提供能力支撑。

目前，蚂蚁链开放存储已支持 MySQL 协议簇和 SQLite 协议簇，满足以上协议簇的关系型数据库存储引擎，可无缝接入到开放存储系统中。此外，开放存储还支持独立于共识主路径的旁路实时写入，适用于区块链数据的读写分离访问模式。在数据一致性方面，开放存储具备保序、一致、灵活回滚的特性，在参与方节点故障时数据库自动被新替换节点接管的能力。同时，蚂蚁链开放存储已获得国产数据库 OceanBase 官方认证，具备对 OceanBase 的良好兼容支持能力。

4.1.4.5 网络

蚂蚁链 P2P 网络服务通过结构化组网、聚合消息路由、纠删码网络传输、用户态协议栈、软硬件融合等技术优化，可支撑百万级消息并发处理能力。

蚂蚁链接入网络服务基于多 CA（认证机构）策略满足多样性网络安全认证需求，支持证书吊销管理；通过恶意请求过滤机制、系统流量控制机制、黑白名单访问控制等技术手段有效保障节点安全运行。

4.2 BaaS 平台增值服务能力

4.2.1 数据洞察能力

链上数据服务基于 BaaS 平台部署的，支持对平台上所有链进行数据获取、数据解析、数据分析等能力。同时，用户可以将链上数据准实时地导出到外部数据系统做进一步处理和分析，实现对链上数据的价值提升。数据服务的产品功能架构如下图所示：



为了让用户能够更好地获取链上数据，并对链上数据做进一步的解析或分析，链上数据服务提供以下两大服务能力：

4.2.1.1 数据导出服务

数据导出服务支持将区块链上特定的区块、交易、合约事件导出到外部的数据系统中，导出过程中保证事件的完整性，符合条件的事件会被推送到外部数据系统至少一次，便于用户对导出后的数据做进一步分析。数据导出服务支持导出指定区块高度区间内的所有事件，也支持持续运行模式，准实时地将链上数据写入到外部数据系统中。外部的数据系统可以是用户的数据库，也可以是一些日志服务等第三方服务。通过数据导出服务，可以避免用户在使用 SDK 方式获取链上数据的不可靠性（如节点重启、网络中断等情况发生时），从而保证能将用户需要的数据可靠地导出到指定的目标里面，用于后续的数据分析。

4.2.1.2 数据融合洞察服务

数据洞察服务支持精准搜索链信息、地址信息、合约信息、交易信息、区块信息等，如具备 ElasticSearch 搜索引擎，还可支持业务数据搜索的能力。BaaS 平台提供数据融合洞察能力，可以更好地解决企业、开发者对链数据的感知需求。通过数据洞察，主要可以实现以下几大功能：

- a. 解决链数据黑盒问题，帮助用户解析、洞察、分析链上数据，辅助业务决策，让链的价值被看见。
- b. 业务数据搜索分析：通过输入您感兴趣的链上业务数据，可以是一个合同的编号、一批农产品的编号），数据洞察服务可以快速地将相关的链上交易筛选出来，并通过对链上数据特征的提取，提供业务决策辅助。
- c. 提供可以互动的链上数据洞察平台，支持用户自定义合约的统计分析，能够对链上数据进行关联打标。
- d. 默认提供更加丰富的链上数据统计能力，支持对链上全量账户、合约的统计和管理。解决开发者在使用当前区块链浏览器时出现的功能不足的问题。
- e. 在数据洞察（ChainInsight）之上，进行数据融合、数据关联分析。
- f. 建立链上数据与链下数据的关联关系，打通业务应用，进行链上链下的融合展示。
- g. 建立链上数据的流动关系，提供链上数据的追踪与分析能力。

4.2.2 跨链连接服务（ODTAS）

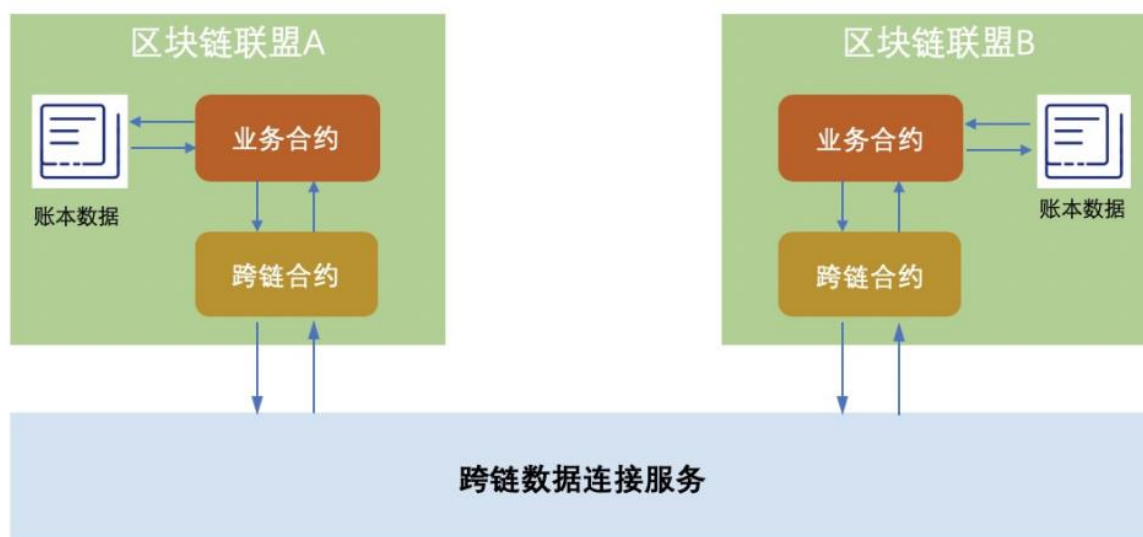
跨链数据连接服务 ODATS（Open Data Access Trusted Service），是由蚂蚁链自主研发的一款面向企业级应用的支持同构/异构区块链之间数据可信交互的服务。

ODATS 是具有超过 30 个专利的自研跨链技术，利用蚂蚁链领先技术，ODATS 制定了标准化的区块链 UDAG 全栈跨链协议，保证跨链交易的安全性、可扩展性及可靠性，打破区块链数据孤岛，实现同构及异构链之间的可信互通，助力企业之间可信协作，促进产业生态可信融合。

4.2.2.1 跨链服务调用链路

使用跨链数据连接服务，需要将区块链在跨链数据连接服务上进行注册。注册过程中，跨链系统会为区块链创建一个区块链域名，该域名在区块链网络中与区块链是相对应

的，可以实现一些账本数据的资源定位。同时，跨链系统会在您的区块链上部署一个系统合约，当您部署业务合约后，会通过业务合约与系统合约交互来完成不同链之间的信息交互。



4.2.2.2 数据交互方式

目前跨链数据连接服务支持两种数据交互方式：

- 账本数据访问：目标区块链能够通过跨链服务直接访问源区块链的相关数据。
- 合约消息推送：源区块链能够通过跨链服务发送消息给目标区块链的智能合约，由目标链的智能合约完成对消息的处理。

4.2.2.3 数据授权方式

跨链授权提供两种授权模式，这两个功能都是基于跨链服务验证、可审计等特性，能够保证信息不会被篡改。

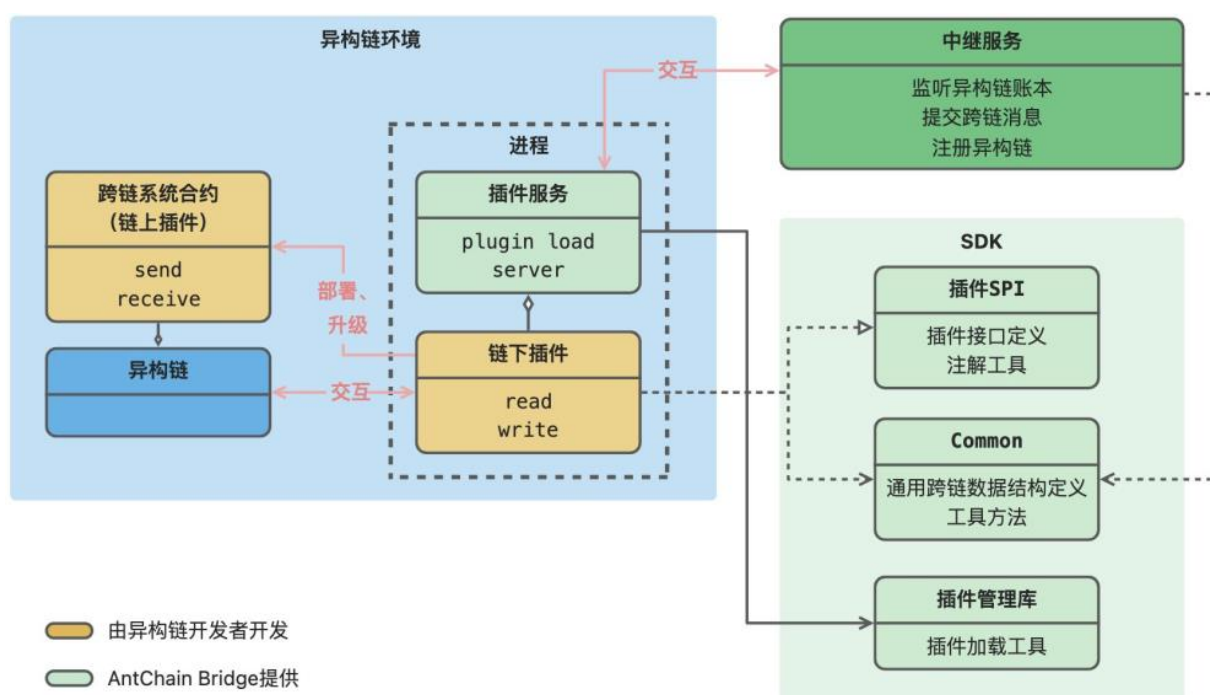
- 账本数据访问：即授权已经注册的另外一条区块链通过跨链服务访问当前区块链的账本数据，可以是一个交易、区块或区块头。
- 合约消息推送：即授权已经注册的另外一条区块链的指定合约向当前区块链的指定合约发送消息。

4.2.2.4 异构链插件化接入

蚂蚁链跨链桥 AntChain Bridge (ACB) 是蚂蚁逐步开源的底层跨链技术和协议。依托 AntChain Bridge 的底层技术，并通过对跨链技术的深入探索和对落地应用的实践积累，蚂蚁链跨链产品 ODATS，已具备成熟跨链互操作能力。

AntChain Bridge 支持异构链以插件化的形式轻松接入跨链网络。异构链的开发者基于 SDK，实现异构链插件，部署插件服务并加载插件，中继和插件服务之间可以通信，就可以将该异构链注册到 AntChain Bridge 中，实现该异构链和其他 AntChain Bridge 支持的区块链的互通。

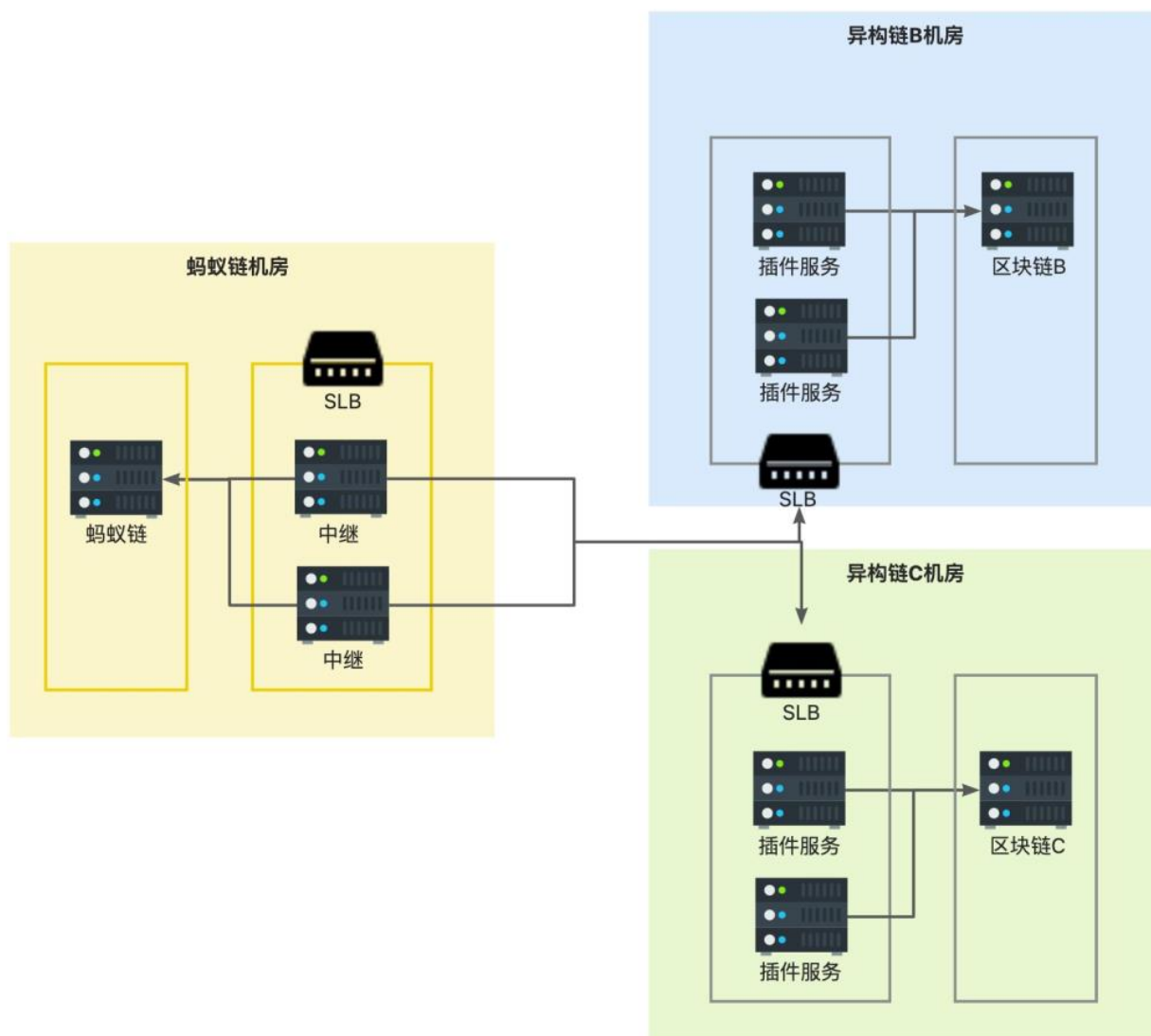
目前，跨链数据连接服务已支持异构链之间的合约消息推送功能，您需要提前开发好对应异构链的插件，开发过程中，需要完成链上插件开发和链下插件开发，异构链插件在整个跨链服务中的具体交互逻辑如下：



- SDK：定义了插件核心的 SPI，提供通用的数据结构以及工具方法。
- 插件服务：一个无状态的 RPC 服务，用于响应中继与异构链的通信请求，插件服务可以通过加载不同异构链插件，实现 SPI 中描述的操作。

- 文档：我们提供了详尽的介绍文档、开发教程和 Demo，您将会和 AntChain Bridge 一起实现异构链接入的 Demo，具体开发流程可参见《开发指南》中异构链插件开发指南。

为了更好地理解 AntChain Bridge 的架构设计，这里给出一个简单的部署架构：



4.2.3 一体化服务平台

平台基于深入的业务抽象，构建了一系列可复用的数据与业务服务模块，包括但不限于数据上链、数据标识、存证、验真、溯源及授信等关键功能。这些模块直击产业痛点，显著降低了应用方的开发成本与技术门槛，加速创新应用的落地进程。平台采用先进的插件化设计理念，实现了服务与智能合约的高灵活性接入，确保业务逻辑能够

快速响应市场变化。通过模块化与合约组件化，平台增强了系统的可维护性和升级便捷性，即便面对区块链底层技术的迭代，也能确保系统的稳定运行与平滑过渡。

一体化服务平台主要功能特性如下：

- **目录与元数据管理**支持用户自定义配置上链目录分支以及相关数据的元数据，方便对上链数据进行分类管理。支持对目录下的元数据进行管理，包括新增、编辑、标识元数据，对元数据确权，启用和删除元数据。新增元数据过程中，支持对业务数据来源，业务数据规则以及上链规则等信息进行配置。
- **数据上链**支持对来源方式为数据库采集的元数据配置上链任务，以此来实现标准元数据的自动采集和上链；同时支持通过接口方式实现数据上链。
- **数据存证**基于数据存证的使用场景广泛应用于区块链技术，平台提供了小文本存证和大文件存证的应用。
- **数据验真**数据验真提供统一的上链数据多场景验真服务能力，验真功能可根据数据内容及哈希值等快速查验。支持用户通过数据标识或待核验数据，以参数组合的形式，自动与已上链的数据进行比对，并返回核验结果。
- **数据溯源**支持授信人员自助使用数据溯源功能，快速追溯数据的全生命周期状态，包含上链时间、当前数据情况、历史变化情况以及数据的字段属性值、可信标识状态等内容。
- **数据授信**提供统一的授信与鉴权管理的能力，针对链上、链外数据进行授信操作，被授信方将有权限访问相关数据。数据所有权方可以新增授信数据，也可以对已有的授信数据进行中止或者做授信时间的变更。被授信方可通过接口方式查询用户名下的授信数据。

4.2.4 多链综合管理平台

多链综合管理平台以信通院发布的政务区块链统一接口规范为基线实现，提供包含路由管理，接入管理以及纳管管理等功能，向下适配集成不同厂商的区块链管控产品，兼容统管不同厂商的区块链技术平台产品，实现多底层链并行。

当政府/企业的环境下存在多个厂商的区块链产品并行运行时，通过多链综合管理平台可以实现对不同厂商的区块链产品进行统一管理。对于企业或部门的开发人员来说，多链综合管理平台能够屏蔽底链的差异，为其提供统一的开发工具，账号管理能力。

多链综合管理平台提供的可视化大屏支持对接入纳管平台的各条链信息进行分别展示，展示信息包括接入联盟链信息、合约信息、业务信息、资源管理信息等，助力企业运营管理人员能够快速响应实时变化的业务数据，从而为业务决策分析提供帮助。

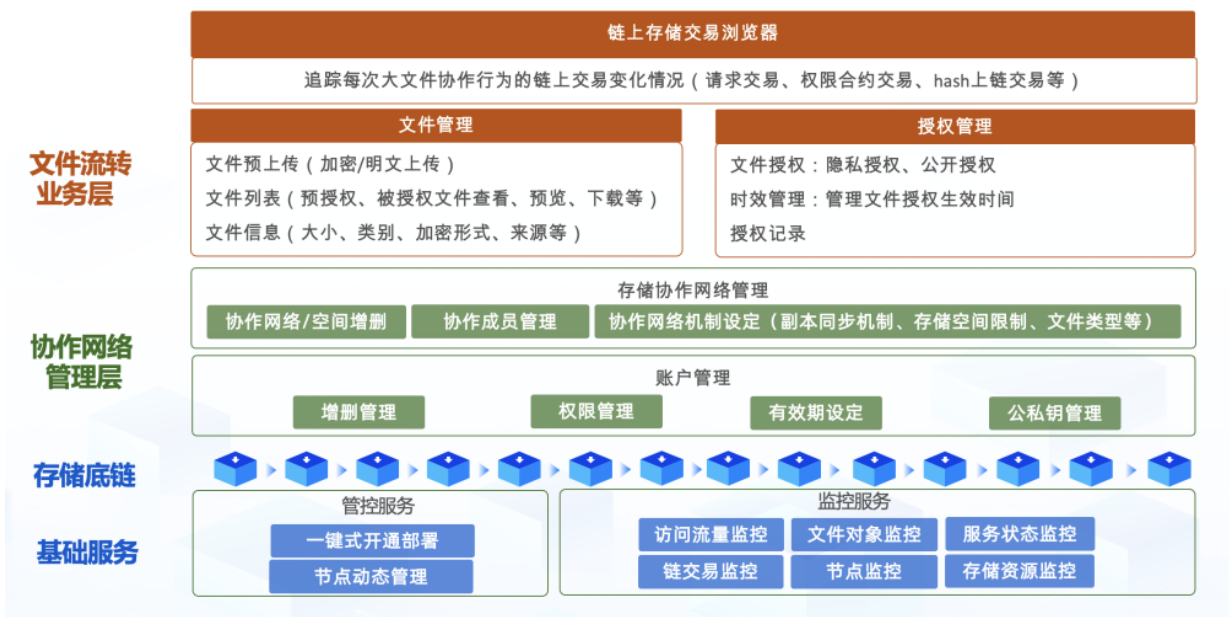
多链综合管理平台主要功能特性如下：

- **机构管理**用户可快速创建机构，并在机构列表下展示所有已创建的机构。同时支持对已创建机构，导入其已有的 BaaS 平台到多链综合管理平台，并在所有机构下展示已导入的 BaaS 平台列表，支持一个机构导入多个 BaaS 平台。
- **区块链管理**在 BaaS 平台列表下，展示所有已导入的 BaaS 平台信息，并支持查看各 BaaS 平台的链基本信息，如块高，节点数、区块链浏览器等。同时支持跳转至各 BaaS 平台控制台，查看并管理该平台内的区块链。
- **数字驾驶舱**提供大屏展示所有已纳管的链的关键信息，如区块链信息、交易趋势、区块信息、实时交易信息、区块链数量、总交易笔数、总合约数、总账户数、区块链引擎分布、总 TPS 趋势、建设案例等。
- **平台用户管理**管理员可以创建多个角色，以便对控制台的各功能点进行权限划分，通过给用户分配角色实现用户隔离，并独立管理。
- **操作日志**提供操作日志，为管理员掌握平台用户的操作权限提供帮助。

4.2.5 多方协同存储

多方协同存储是融合区块链、数据加密、隐私保护、P2P 网络共享传输等技术的去中心化存储产品。多方协同存储主要面向多方协作之间数据流转和共享的场景，提供安全、高性能、稳定可靠、组网灵活的协同解决方案。例如，在政府、金融、运营商等行业的数字化协作应用场景中，多方协同存储可满足越来越多的关于数据安全分发、共享传输、就近获取等的应用诉求。

多方协同存储，采用分层的产品架构，结合区块链的多方共识信任的特性，构建多参与方、多地域、分布式的去中心化存储服务网络。如图下所示：



- **基础服务：**包括管控和监控两部分，主要面向运维等技术角色，作为基础能力，提供配套的系统服务和故障感知保障。
- **存储底链：**技术架构上，引入区块链作为信任保证的支持设施，实时跟踪存储流转和管理的过程，提供透明、无纠纷、共享的保障。
- **协作网络管理层：**承担多参与方的协同服务能力，包括协作成员管理，协作空间管理和隔离，协作网络机制设定等。
- **文件流转业务层：**由核心存储引擎承担，提供数据和文件高性能存储和分发的基础能力，同时开放数据授予和隐私管理。
- **链上存储交易浏览器：**承担数据面板的服务，实时跟踪存储协同交易，文件数据的分发流转，以及关键数据的汇总统计。

4.2.6 区块链传输网络（BTN）

BTN(Blockchain Transmission Network)是区块链网络的“数字高速公路”，支持蚂蚁链及其他区块链建立规模化应用。BTN 通过智能路由算法、高效传输协议、传输优化、

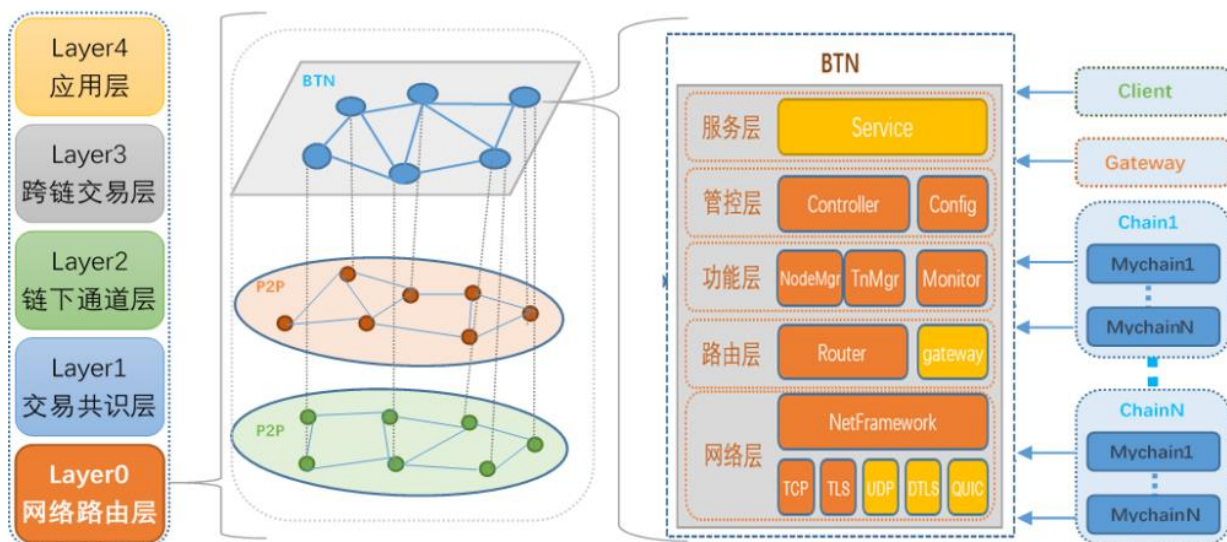
虚拟网络专线等技术，提升区块链节点连接的连通性、稳定性和实时性，实现全球区块链网络的高速、安全互连，是支撑区块链规模化、生态化发展的公共网络基础设施。

去中心化 P2P 网络是区块链系统中多节点间协议交互通信的基础，用以承载区块链系统中交易广播、共识通信、数据同步等数据交互协议，数据传输模式主要为广播或者组播。蚂蚁链在大规模复杂异构网络环境下有丰富的沉淀与技术积累，通过多层次立体化的网络架构设计，在骨干、边缘、应用等多个层次构建了灵活高效组网能力，提出并实现高速传输网络、高性能安全网络服务、按需动态组网等技术，推出 BTN 产品，支撑区块链大规模高质量网络组网、灵活网络拓扑管理、高性能网络通信、多业务网络灵活协同等复杂业务需求。

4.2.6.1 核心功能

区块链传输网络（BTN，Blockchain Transmission Network）是蚂蚁链为了解决区块链实际应用场景下的挑战而提出的网络优化解决方案。传统区块链节点面向全球部署时，节点之间通过 p2p 通信，时延高、抖动大，网络很不稳定。另外联盟链往往对节点通信的安全性要求较高，节点间需要彼此开放白名单，这导致在一个联盟中新增联盟节点的时候需要推动已经存在的所有联盟节点升级白名单。面对上述挑战，BTN 在区块链的 layer0 层建立一个多链共享的区块链通信网络，提升区块链节点的网络稳定性、连通性、实时性的同时，解决联盟链成员变化彼此需要升级白名单等用户痛点。

BTN 网络是区块链节点通信的骨干网络，可与区块链 p2p 网络共存。在保持区块链节点对等性的基础上，构建了底层低延时传输能力，应用层灵活的消息路由能力，业务层的高并发服务能力，可以给区块链应用提供工业级的服务和运维保障能力。



BTN 网络在全球部署了几十个区域节点，区块链节点及 DApp 可在任意位置就近接入。BTN 网络应用组播消息聚合、边缘复制、实时多路路由、应用感知加速等技术实现了低延迟、低带宽、高可用、高可靠、可运维、业务无感的区块链通信网络。

4.2.6.2 产品优势

- 面向全球部署，把实时通信 (RTC) 技术和区块链业务特征结合，实现区块链实时通信，提升区块链交易速度和吞吐量。
- 通过自定义协议实现广播、组播消息聚合，大幅降低区块链节点带宽消耗。
- 创新的应用感知加速技术，保障区块链消息的实时性，提升了链性能。
- 灵活的应用定义快速路由算法，支持异构区块链共享同一个 BTN 应用加速网络。（支持蚂蚁链、Fabric、金链盟 BCOS、比特币、以太坊等主流联盟链和公链通信）。
- 中立的边缘代理节点，联盟成员变动无需对已经存在的联盟成员进行安全访问策略的升级。
- 任意节点双 region 级别容灾，升级过程用户无感知，不影响业务。

4.2.6.3 技术能力

区块链传输网络是一个面向去中心化通信场景，支持多链多应用共享，支持安全通信的区块链传输骨干网络，用于解决大规模区块链节点（或 DApp）P2P 通信效率低、稳定性差，难以支撑工业级生产应用的问题；同时为区块链应用生态构建基础设施，支持大规模去中心化应用和节点之间的任意互通，支撑区块链服务的稳定性、弹性和访问便捷性。BTN 网络可以为业务提供三种技术能力：

- **高性能传输能力。**BTN 提供快慢通道，支持实时型和流量型两种通信流量特征，保障实时性；通过广泛部署接入点，实现就近接入，缩短公网路径，提升网络稳定性保障。
- **多业务承载能力。**支持大规模区块链、DApp 节点实现 P2P 互通，快速形成多业务协作网络，还支持 CS、BS 通信业务，通过 BTN 轻松实现交易上链、信息查询等。
- **跨网闸安全通信能力。**全链路 SSL 加密，保障传输层安全；mTLS 方式身份验证，保障节点身份不会被仿冒。

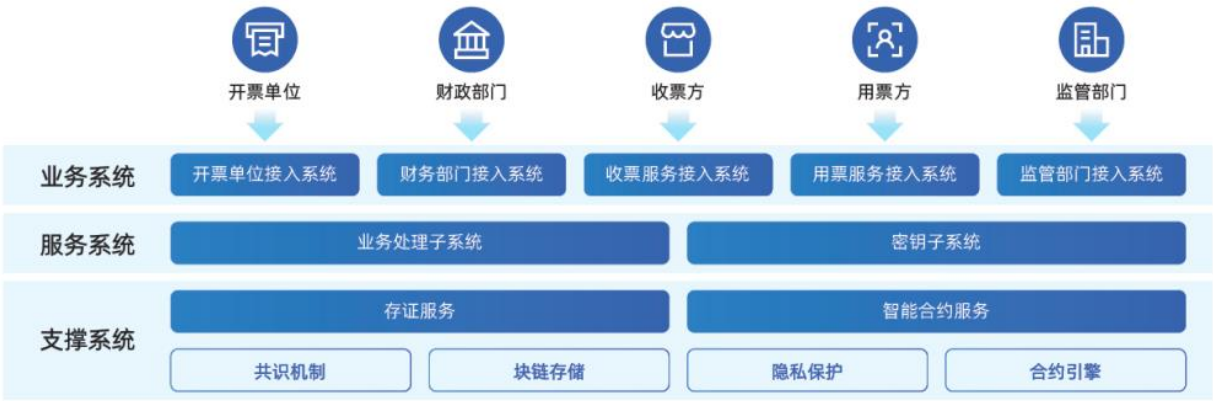
5. 典型案例

5.1 案例一：浙江省电子票据管理中台

浙江省区块链电子票据平台是全国首个区块链电子票据平台。根据“最多跑一次”改革和政府数字化转型要求，省财政厅联合省卫生健康委、省医保局、省大数据局共同推进医疗收费电子票据改革，借助区块链、云计算、大数据等先进技术，聚焦老百姓看病报销“一件事”，在破解“看病烦、报销慢、监管难、成本高”等方面取得实质性突破。

支撑系统主要通过区块链的共识机制、块链存储、隐私保护和合约引擎提供存证服务和智能合约服务。服务系统包含密钥子系统和业务处理子系统，其中密钥子系统负责密钥管理和密钥生成，业务处理子系统实现票据上链、查询、理赔、报销等业务的处理。业务系统提供接入系统，用于服务使用方发起业务。

其中，医疗电子票据中蕴含大量个人医疗敏感信息，因此数据保护是我们工作的重中之重。使用区块链技术协调解决多部门间的信任协同机制，使原本割裂的电线之间形成网络效应，逐步建立各级财政部门与各部门、各执收单位、浙里办等联网信息共享机制，打破“信息孤岛”。加强对财政电子票据生命周期的监督，确保电子签名签章文件的合法有效、安全传输、安全储存，保证票据开具的规范性、安全性。



5.2 案例二：浙商中拓工程配送项目

浙商中拓携手蚂蚁数科、阿里云，共同打造工程配送可信数字化平台。利用区块链、实人认证、电子签名、可信存证等数字科技，实现业务全流程线上化和行业数据共享，提升各方业务互信。

该项目由工程配送物流系统和行业数据对接平台组成。其中，工程配送物流系统主要包含以下三项功能：

- 通过物流管理系统+小程序实现司机和签收方的线上化协同，减少信息重复录入和低效的纸质单据线下传递；
- 车辆轨迹追踪实现运输全程监控；
- 实人认证和电子签名保证交接人的真实性，避免被冒名顶替。

行业数据对接平台具备以下能力：

- 标准接口：连接供应商、贸易商、物流公司、仓储公司等服务对象，制定行业上下游数据对接标准接口，提升行业标准化水平。
- 高效溯源：引入区块链溯源平台，推动关键业务节点数据上链存证，如配货单、出库单、运单、签收单等，上下游数据交叉验证，佐证业务数据真实性，实现建材使用全生命周期链上追溯；当发生工程事故追责时，高效完成责任追溯。
- 过程增信：提升线上化监管能力，为后续金融业务风险防控打下数字化基础。



5.3 案例三：GSBN 无纸化放贷项目

GSBN 基于区块链构建“无纸化放贷”应用，为客户提供无纸化、高效和透明的解决方案，将航运生产上下游各方链接成一个高效、可信的生态系统。

首先，数据共享。基于区块链技术和密码学，GSBN 的成员可以放心地分享数据而不必担心数据泄露或未经授权的使用。通过与领先的航运班轮公司和码头联盟的合作，GSBN 还可以确保所使用的数据标准适合相关行业并被行业所采纳。

其次，应用创新。通过使用 GSBN 上的 API，会员可以创建新的应用来改善业务流程，降低成本和设计全新产品。目前，客户可以在区块链上一次完成贯穿船公司和港口的

操作流程，实现全流程无纸化，放行所需时间从几天缩短至几小时，满足物流交付时间和货物跟踪精确到小时级的要求。同时，GSBN 进一步研发了电子提单产品，助力产业链数字化升级。通过 GSBN 的区块链基础设施，电子提单全程依托区块链技术，实现全面数字化、私有化和独特性，从根本上规避了纸质货单容易丢失、假冒及涂改的风险，提高国际贸易中运输文件的数字化水平。

基于电子提单，银行、金融机构将放货手续时间由之前的 24 小时至 48 小时，缩短至现在的 4 小时以内，融资效率提高，从而为航运行业提供更多贸易融资的机会以及更好的服务体验。





蚂蚁集团
ANT GROUP

数字科技