蚂蚁链

区块链服务平台
产品简介

产品版本：V3.1.1

文档版本：20250314

蚂蚁集团
ANT GROUP

法律声明

蚂蚁集团版权所有©2022，并保留一切权利。

商标声明

免责声明

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.产品概述

本节通过蚂蚁链对蚂蚁链私有化标准版做整体性的介绍。

区块链是一个典型的分布式协同系统，多方共同维护一个不断增长的分布式数据记录，这些数据通过密码学技术保护内容和时序，使得任何一方难以篡改、抵赖、造假。区块链根据不同需求和场景可分为公有链、联盟链和私有链。

蚂蚁链以联盟链为目标，突破商业与金融应用场景，率先实现了具有高可靠性、高可运维性、高安全性和适配全球部署等优势的工业级与金融级区块链系统，并已在存证、跨境汇款等最初应用基础上逐步实现了政务、金融、低碳、公益等超过50个场景的落地应用。

区块链 BaaS（Blockchain-as-a-Service）平台依托蚂蚁链平台，提供技术领先的区块链服务。该平台具备简单易用、一键部署、快速验证和灵活定制的特点，可加速区块链业务应用的开发、测试和上线，助力各行业区块链商业应用场景的落地。同时，该平台具备高性能、稳定可靠、隐私安全以及多种类型数据的区块链存证能力。

蚂蚁链 BaaS 平台基于蚂蚁自主研发的区块链引擎，构建了强大的区块链底层架构。该平台经历了重要的升级，以支持智能合约和大规模产业化应用。最初的阶段主要服务于政府公共服务和金融创新，通过通用智能合约平台满足多样化的业务需求。随着区块链技术和应用的飞速发展，平台架构不断完善，以适应大规模组网、分层治理和扩展性的更高要求。这一能力提升标志着从支持单一场景到满足复杂业务生态系统的转变。

蚂蚁链 BaaS 平台基于蚂蚁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。

2.产品优势

蚂蚁链私有化标准版有其自身的功能特点，本节重点介绍其各方面性能和优势。

BaaS 平台优势

作为行业领先的区块链服务平台，蚂蚁链私有化标准版 BaaS 平台具备以下优势：

高性能

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网络部署区块链节点，即参与共识的节点可以运行在用户各自的 IT 环境，也可以运行在公共云平台上。

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，只需在已提供的相关资源环境上运维即可，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。

蚂蚁链区块链引擎 核心优势

BaaS平台的核心蚂蚁链区块链引擎能够为您的业务系统提供更高的性能和安全性，同时有效降低使用及运维成本。

更高性能

蚂蚁链区块链引擎在自适应交易并行调度、计算存储分离的架构和高效的区块并行流水线方面进行了改进，相比之前系统性能得到了显著提升。

- **自适应的交易并行调度** ：结合数据模型与并行调度算法，自动识别并行执行交易的可能性，有效提升交易处理速度，同时确保区块执行的一致性。
- **计算存储分离的可扩展架构** ：把计算与存储分离，允许计算资源和存储资源根据需求独立横向扩展，提高系统性能和容错能力。
- **高利用率的区块并行流水线** ：通过优化区块处理流程，通过流水线的方式，实现区块在不同处理阶段的并行调度，大幅度提升系统吞吐量。

多维扩展

蚂蚁链区块链引擎旨在提供具备安全性、灵活性与高性能的区块链解决方案。除了高效安全的共识算法，灵活可变的组网方式，单个共识节点内的可扩展并行架构是获得高性能的基础。我们通过计算存储分离的服务化架构，自适应的交易并行调度、高效的异步流水线调度从多个维度提高了单节点的扩展性，并利用单机分布式一体化的设计，既支持简单易用的轻量化部署，同时又能按需扩展，平滑扩容。

并行架构

并行架构的设计旨在充分利用单机多核处理能力和多机集群的扩展优势。然而，区块链系统在考虑系统的扩展性时，需要从更多维度来考虑，其中包括保证执行一致性的交易并行策略，以及确保协议安全的区块异步调度。蚂蚁链区块链引擎的多维并行策略主要体现在计算/读写并行、区块间并行和区块内并行三个方面。

大规模共识与协作网络

蚂蚁链区块链引擎凭借自主研发的MyTumbler共识协议、灵活的动态子网机制、立体化的网络架构和BTN加速服务，实现了大规模网络下的高效共识、高度可扩展性、数据隐私保护及网络通信优化，为企业级区块链应用提供了强大的基础设施支持。

可验证多模链存储

蚂蚁链区块链引擎凭借自主研发的一系列核心技术，包括Merkle Trie Tree数据结构、LETUS高效可信通用存储引擎、分布式存储服务体系MyGrid，以及创新实施的区块数据动态冷热分层策略、Snappy压缩算法实现的区块数据动态压缩，和状态数据智能动态裁剪机制，显著提升了存储效能与成本效益比。这些综合技术不仅确保了数据的高安全性、可验证性和存储效率，还通过精细化管理和技术优化，实现了存储资源的最优化配置和成本的有效管控，为大规模区块链应用奠定了坚实的存储基础。

全方位安全体系

蚂蚁链区块链引擎从多个维度和视角出发，为区块链系统提供了全面的安全保障。通过集成先进的密码学组件、采用严格的链节点准入机制和通信机制、设计独有的账户与交易规则、融合自研的合约执行引擎，从而构建了一个多层次、全方位的安全架构，充分保障了系统和用户的安全需求。

3.功能特性

蚂蚁区块链私有化标准版提供简单易用，一键部署，快速验证，灵活可定制的区块链服务。

联盟链创建

用户可以在产品控制台上传许可证和区块链安装包，指定运行区块链节点的各个服务器地址后，自动化建链。

联盟链管理

用户可查看联盟链的节点信息，包括节点地址，服务端口，共识状态等信息。也可指定服务器地址，自动化添加域内/域外节点，另外还支持创世配置、升级联盟链版本的操作。

节点管理

用户可以查看节点的地址、运行状态、共识状态、区块缓存队列、交易缓存队列、节点块高等信息。也可以操作节点重启、停服/启服、节点配置信息修改、SSH配置信息修改、节点共识状态更新、节点名称修改，以及节点证书更新。

证书与账户

用户可在控制台上创建应用程序访问区块链所需的SSL连接证书和私钥。以及发起交易所需的区块链账户（公私钥对）。

智能合约集成开发工具

控制台提供简单、高效的合约集成开发环境（IDE），帮助开发者进行合约的编辑、编译、部署、调用、单步调试、单元测试、自动编解码等。

应用开发组件

提供Java SDK，可覆盖蚂蚁区块链所有功能。同时提供稳定、高性能的REST接入服务，较SDK简单易用，降低用户上链应用的开发成本。

区块链浏览器

可通过区块链浏览器查询交易数目，节点信息、最近出块信息、块中包含的交易信息、区块信息查询、交易信息。

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，最终完成用户隔离，并独立管理。

子网能力

提供在主链上创建子链的方案，实现一条链上可以运行多个业务，并且做到不同业务的参与方不同，从而达到数据隔离的效果，方便业务方更灵活的架构自己的业务、节省成本。

在此基础上，还支持跨子网数据查询和合约读操作，具体在**《开发指南》**的**跨子链通讯**章节中有详细的介绍。

软件许可管理

提供对授权节点所需的软件许可文件进行统一管理的能力，支持用户查看软件许可文件的过期时间、已使用/未使用的节点授权信息等，帮助用户合理使用节点授权文件。

健康管理

健康管理模块提供以下几大能力，通过这些能力可以确保区块链网络的稳定、高效运行：

- 健康视图

  通过分析区块链网络的运行特征，展示宏观的健康状态，并提供自治功能的使用建议。

- 自愈恢复能力：

  系统能自动感知、诊断并恢复常见故障，提高故障解决效率，降低运维成本。
- 流量分析能力

  实时监测区块链的流量使用情况，包括流量状态、峰值、偏差时长、负载承受度等。
- 资源监测能力

  使用动态预测技术分析资源瓶颈，实时监测节点的CPU、内存、存储及网络带宽使用情况。
- 参数诊断能力

  自动分析区块链网络的运行状态和交易特征，提供优化点和风险点的诊断建议。
- 成本评估能力

  评估区块链基础设施的运行状况，提供成本优化的建议，帮助用户节省资源使用成本。

4.蚂蚁链介绍

蚂蚁链通过引入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。基于蚂蚁链提供的能力和功能特性，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。

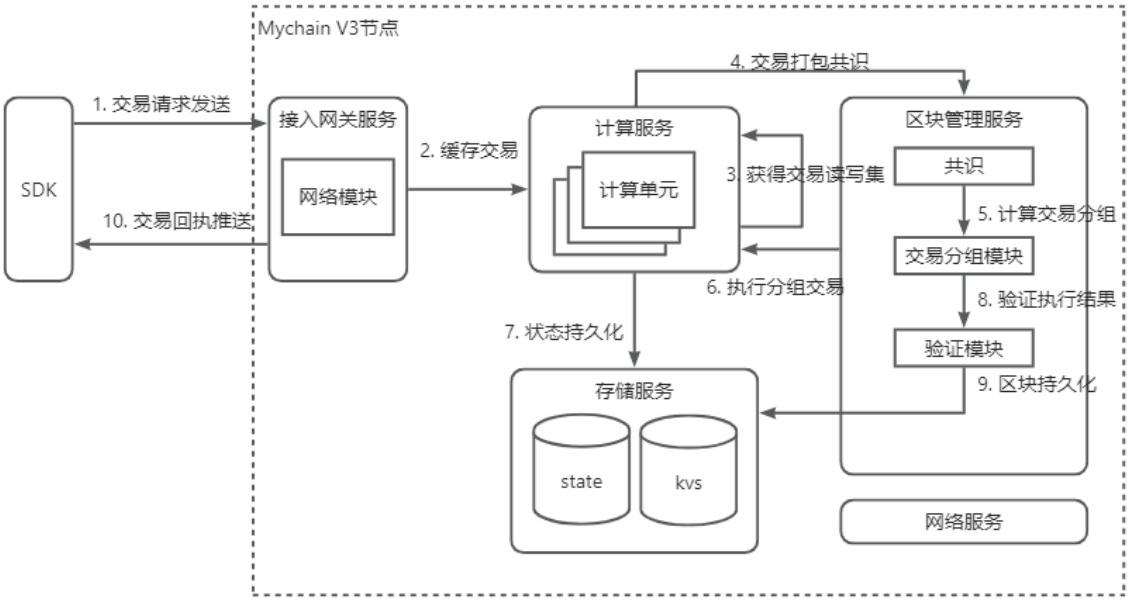
逻辑视图

MyChain V3平台通过创新的技术架构设计，旨在提供高性能、灵活性和安全性的区块链解决方案。平台由六个核心服务构成，包括接入网关、计算服务、区块管理、子网容器、存储和网络服务，这些服务通过模块化设计和服务化框架实现高效协同工作。MyChain V3支持单机分布式一体化架构，既能满足高并发、大规模的业务需求，也能通过Lite模式提供低成本、易部署的解决方案。

MyChain V3由6个核心服务构成，其中无状态服务（如计算服务，子网容器服务），可通过水平扩展从而提升吞吐率，另外有状态服务可通过分片扩展的能力（比如存储服务）提升吞吐率的能力。区块管理服务由于本身需要协调各个服务之间的行为和工作，因此并没有做成分布式可水平扩展的服务，但是在实现上可支持主从切换的能力从而保证高可用。

- **接入网关服务：** 负责处理跟SDK的连接管理和消息传递，支持http和原生协议两种通信方式，并且具备一定的流控能力
- **计算服务：** 负责缓存待处理的交易，以及对这些交易进行合法性验证以及预执行得到读写集。以及最后根据分组结果进行交易的实际执行。这个模块本身无状态，可以水平扩展
- **区块管理服务：** 用来协调整个区块的生命周期，包含关键的区块调度能力，是整个系统的控制中枢
- **子网容器服务：** 用来在pro模式下管理多个子网实例的服务，主要功能包括服务托管以及对应请求的代理转发
- **存储服务：** 负责所有需要持久化数据（状态，区块等）的管理，支持数据分片的能力，从而支持水平扩展提升性能
- **网络服务：** 主要包括domain之间的消息交换和传递，支持多种通信模式以及增强的通信网络BTN
- **统一服务化框架：** 主要是用来协调各个服务之间通信的框架，主要包括远程调用、服务注册，配置管理等

流程视图



1. **交易请求发送：** SDK根据MyChainV3协议构造对应的交易原文并且进行签名，发送给任意一个区块链节点
2. **缓存交易：** 接入网关服务收到SDK的交易后，对交易的合法性做相应检查，检查通过的交易放入计算服务的缓存模块中
3. **获得交易读写集：** 对交易的签名，重放攻击等以及有效性进行校验，并通过预执行得到该交易的读写集
4. **交易打包和共识：** 通过有效性校验和产生读写集之后的交易进行按批次打包，共识
5. **计算交易分组：** 按照读写集进行交易分组
6. **执行分组交易：** 根据分组的结果，执行对应的交易，如果发现有冲突，重新到5，否则进行下一步
7. **状态持久化：** 修改的状态集合在世界状态(state)上保存
8. **验证执行结果：** 确认跟其他节点的执行结果（区块头中包含的信息，比如世界状态，收据集和交易集等信息），产生共识证明
9. **区块持久化：** 区块头，区块体以及对应的元信息（块高，交易索引）等进行持久化保存（kvs）
0. **交易回执推送：** 给SDK返回对应的交易执行结果

功能特性

账户模型与状态转换

蚂蚁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。

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。

- **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，目前提供对 EVM、Native、MYVM、Precompiled 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。

- **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。

链原生数据管理系统

蚂蚁链具备以下存储能力：

- **数据存储**

  数据存储分为本地文件系统的 KV 数据库存储以及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。

- **世界状态存储**

  蚂蚁链中，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，为合约状态以及世界状态提供了唯一稳态 Hash 值的计算，同时支持树上节点快速索引、更新。

- **历史数据**

  蚂蚁链中，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，进而查询到不同历史状态下的数据。

共识协议

在蚂蚁链中，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共识协议。目前，蚂蚁链系统中已实现的共识算法包括 PBFT共识算法和MyTumbler异步共识算法。

- **PBFT（Practical Byzantine Fault Tolerance）共识协议**

  能容忍系统中不超过 1/3 的拜占庭节点，在此基础上还能保证任意数量的诚实节点宕机重启后的状态一致性。该协议通过 PrePrepare、Prepare、Commit 的三阶段提交协议来达成共识。蚂蚁链提供的 PBFT 共识插件支持使用交易哈希进行共识，以及对大消息使用纠删码广播的技术，降低网络带宽消耗，提升共识效率。此外通过确定性的状态持久化确保异常节点恢复后状态的一致性，防止分叉的可能性。

- **MyTumbler异步共识协议**

  MyTumbler共识算法是我们自主知识产权的新一代更高效、更灵活的异步共识算法，同时也作为MyChain V3中的默认共识算法。相关理论成果被发表在操作系统顶级会议SOSP'23上。这是一种在**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。

PBFT 和 MyTumbler 共识算法特性对比如下：

共识算法	优点	缺点	使用场景

PBFT	• 1/3拜占庭节点容错，任意数量宕机恢复容错。 • 正常无错情况下延迟低，三轮消息交互完成共识。	• 依赖单一主节点提案，节点带宽使用不均衡。 • 如果主节点异常会触发超时换主流程，会造成短暂性能波动。	4~100共识节点，网络环境稳定、高性能场景。
MyTumbler	• 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。	4~100共识节点，公网大规模集群，尤其是广域网、高带宽、高延迟的网络以及不稳定的网络。

> **说明**
>
> 目前蚂蚁链可以根据网络情况和集群情况流畅地在PBFT 和 MyTumbler 共识算法之间进行动态共识切换，具体可在链的**创世配置**中进行配置。

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链状态机抽象模型的全局状态的更改方式。

考虑到大部分用户对以太坊合约比较熟悉，同时又有部分用户对智能合约的执行性能有较高的要求，MyChain V3提供了两种链上虚拟机类型：

- **以太坊兼容的EVM虚拟机**

  提供与以太坊完全兼容的EVM虚拟机，旨在为开发者提供一个熟悉、易用的开发环境，开发者可以无缝移植现有以太坊合约，无需进行任何代码修改。

- **AntVM虚拟机**

  AntVM JIT编译器是AntVM智能合约虚拟机的一个子模块，它使用JIT技术将WASM字节码编译为机器指令，为用户提供智能合约的极致执行效率。

蚂蚁链自研的AntVM虚拟机具有如下特点：

- **高性能：** 相比传统的WASM解释执行虚拟机，AntVM 的执行速度可以提高数倍甚至数十倍。
- **确定性：** AntVM 在 WASM 1.0 spec 的基础上设计了确定性相关的扩展 spec，排除了不同实现方式或者不同 CPU 架构下带来的隐藏的不确定性。
- **兼容性：** AntVM 支持多种编程语言，包括 Java、C++、Go 等，满足不同开发者的需求。

安全机制

MyChain V3在设计和实现过程中，综合考虑了区块链系统各个方面的安全需求，致力于提供一个高度安全、可靠和高效的区块链平台。其安全机制涵盖了账户安全性、交易安全性、网络安全性、共识安全性、客户端准入、合约安全性以及节点灾备和恢复等多个维度，确保系统在各种攻击和故障情况下依然能够正常运行。

- **账户安全性：**

账户的安全性主要体现在基于私钥的签名机制进行账户操作确权。MyChain V3默认采用ECC椭圆曲线（Secp256K1）及ECDSA签名算法，同时兼容Secp256R1/RSA2048和国密算法SM2，为账户操作提供多维度安全保障。MyChain V3的账户在隐私保护的场景下，支持同态加密和零知识证明实现账户金额的隐藏。MyChain V3还设立了账户重置密钥机制，即使私钥遗失也能通过安全流程恢复账户访问，增强了账户的可持续性和可靠性。

- **交易安全性：**

  MyChain V3通过综合运用账户公私钥及交易签名、交易时间戳的对比、随机数及双重验证（前置验证与后置验证）等策略，从多个维度保障交易不可伪造、不可重放以及合法性，确保交易处理的高度安全与一致性。

- **网络安全性：**

  客户端和节点通过 CA 中心获取 TLS 证书，客户端与节点、节点与节点间实行 TLS 双向认证，且通信流量经 TLS 加密，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。MyChain V3还针对作恶节点予以限制，基于节点来配置有效的黑白名单机制，只有通过黑白名单校验的接入方才可以建立有效的链路；针对异常的消息报文进行检测，对于非法的协议消息报予以拒绝，并对请求方的链路予以断开。

- **共识安全性：**

  蚂蚁链的共识算法的容错性比传统的 1/3 拜占庭容错性更强，具备更高的安全性。具体体现为，蚂蚁链不仅能容忍系统中不超过 1/3 的拜占庭节点，在此基础上还能容忍任意数量的诚实节点宕机重启错误，并保证重启后的状态一致性。

- **客户端准入：**

  在默认情况下，MyChain V3节点并没有针对用户进行权限管理的方式，用户申请了通过CA颁发的有效身份证书后，就可以连接到所有节点。同时，MyChain V3也支持通过证书准入规则，用户（管理员权限及Administrator账户签名）可通过手动在节点上添加黑名单配置来设置账户黑名单，以此来限制客户端连接到节点上。

- **合约安全性：**

  MyChain V3通过集成EVM以及自研的AntVM引擎来完成对智能合约执行，支持同一个区块内多个交易的并发执行，每个引擎彼此之间相互隔离，不受合约彼此执行的约束和影响；通过Gas机制来实现对智能合约执行复杂度的衡量。通过上述机制确保智能合约的运行时调用的指令限制在有限的范围内，以防止用户写出无限循环的代码智能合约代码 ；同时，平台提供基本的权限校验和控制能力，能够有效控制合约调用方的权限，只有在合约内指定的账户方可发起特定的合约调用操作。

- **节点备灾和恢复：**

  MyChain V3不同共识节点支持多机房部署方式实现业务容灾能力，确保在单个机房出现故障等情况下保持数据的完整性和业务的高可用，但由于区块链的BFT特性要求链上大多数共识节点的投票才能完成正常的共识逻辑，无法将链上共识节点分配至多机房达到任意机房故障时的容灾目标。MyChain V3同时支持利用非共识节点、网络全连接的特性，通过增加非共识节点作为共识节点的热备节点方式实现链整体的灾备功能；通过节点身份切换（共识->非共识，非共识->共识）能力保障当共识节点运行异常导致链停止出块时，可以分钟级恢复链的正常运行。

可信执行环境与跨链技术

蚂蚁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。蚂蚁链使用可信计算环境打造可以外部数据调用的 Oracle 集群，解决区块链协议只能访问链上数据的局限性问题。

信任构建与系统治理

蚂蚁链联盟的信任构建机制主要有创世信任、基础信任、共识信任、输入信任、治理信任、可验证信任。这些信任构建机制共同建立了蚂蚁链联盟的高度可信任的特征。

蚂蚁链提供联盟管理能力，即对具体区块链联盟的成员结构的治理能力。

其他特性

国产化

蚂蚁链已适配主流国产化软硬件环境，获得多家国产厂商互认证书。

- 支持国产CPU列表：
  - 腾云S2500处理器
  - 海光5000系列处理器
  - 海光7000系列处理器
  - KH-30000系列处理器
  - KH-20000系列处理器
  - ZX-C系列处理器
- 支持国产操作系统列表：
  - 银河麒麟服务器操作系统（飞腾版）V10
  - 银河麒麟服务器操作系统（鲲鹏版）V10
  - 统信服务器操作系统V20

国密算法

国密算法即国家密码局认定的国产密码算法，包含SM2、SM3、SM4等。蚂蚁链自主研发通用密码学框架可定制化快速适配各种密码学算法，已支持国密SM2椭圆曲线公钥密码算法、SM3杂凑算法、SM4对称加密算法。

双层密钥体系

设计上采用双层密钥体系，防止TLS证书与签名使用同一私钥带来的安全隐患：

- 通信密钥：基于PKI证书体系采用双向认证的网络安全链路方式，防止信息的泄漏，确保数据传输的安全性。
- 签名密钥：独立的账户模型结合密码学的安全性能够很好的完成账户身份的认证、交易的防篡改、交易的防双花。

网络压缩

为了提升区块链系统网络通信效率，蚂蚁链支持基于Zlib的网络通信数据的压缩功能。该功能主要是针对大数据报文的发送、接收的需求，可根据带宽等需要开启压缩功能，通过发送方压缩、接收方解压的方式减少网络通信数据量，在高吞吐或高数据量的场景下，可节省40%左右的带宽占用。

5.支持跨链服务

蚂蚁链私有化标准版已支持对接跨链数据连接私有化服务，跨链服务支持同构/异构区块链之间数据可信交互的能力。

什么是跨链数据连接服务

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。

> **说明** 更多关于跨链数据连接服务的介绍，请参见**《跨链数据连接私有化服务 》**产品中**技术白皮书**的内容。

跨链服务的能力

> **重要** 您在中途岛平台上使用跨链服务前，需要先在平台上注册具有跨链权限的账号，并开通跨链服务，才能体验跨链服务。详情请参见**《跨链数据连接私有化服务》**产品中**用户指南**的相关章节。

目前跨链数据连接私有化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。

> **说明** 了解更多跨链相关的操作，请参见**《跨链数据连接私有化服务 》**产品中**用户指南**的相关章节

使用场景

您可以将中途岛平台上创建蚂蚁链，与其他平台上创建的链（例如符合Fabric标准的链），实现异构跨链的数据交互场景。

6.应用场景

本节举例介绍了蚂蚁链在各行业中的应用场景。

公益慈善

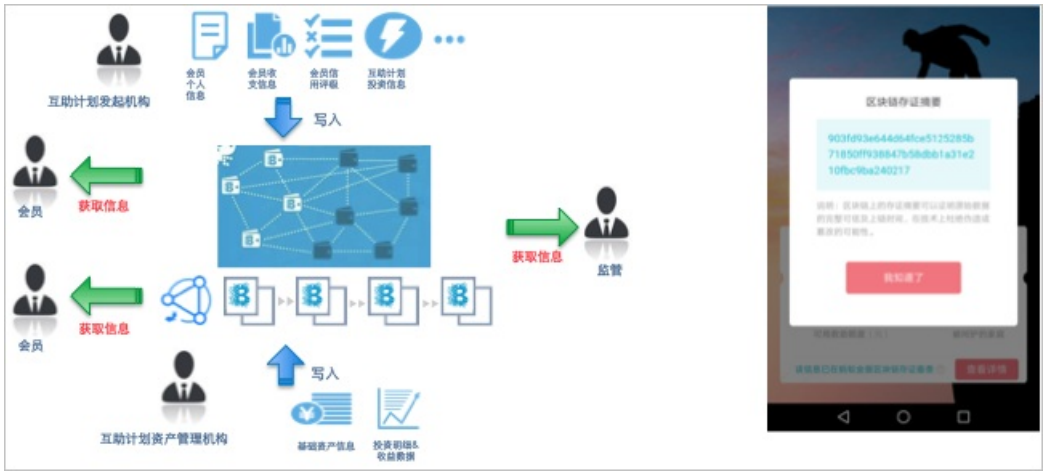
截止2017年07月，上线1年，累计有38家公益机构、355个公益项目上链。

天猫溯源

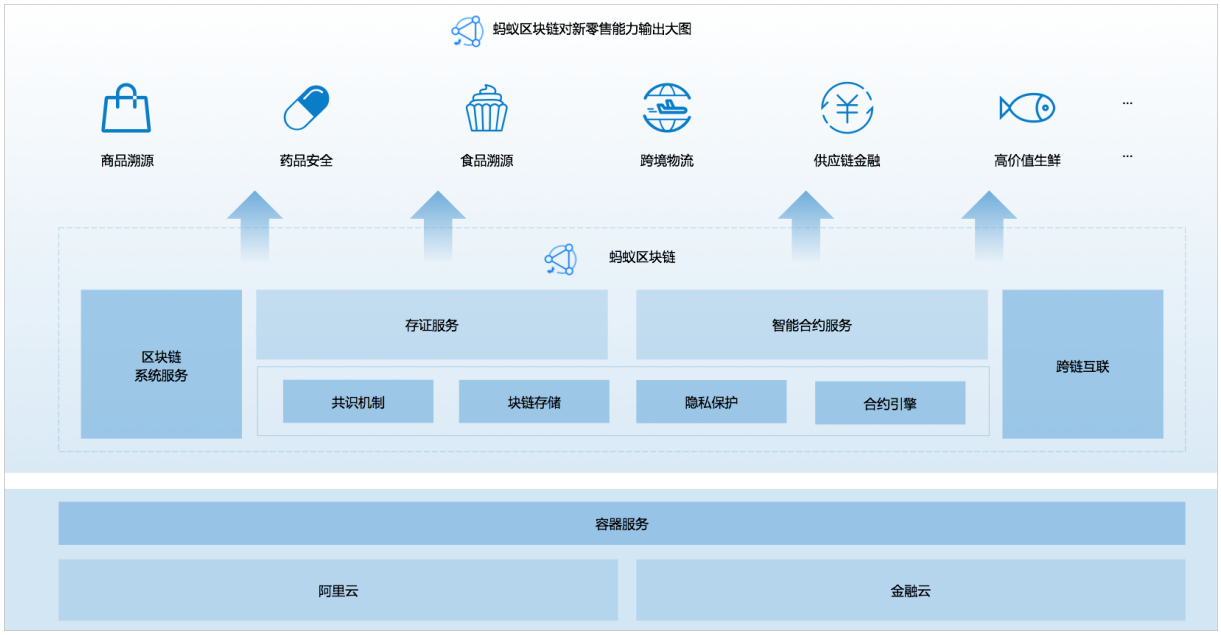
- 目前有3个品类，6000万+件单品
- 手淘/支付宝扫一扫查溯源信息

互助保险

- 提升互助计划透明度，增加会员的信任度
- 赋能机构提升自律披露水平，配合监管


互助计划发起机构
写入
会员
获取信息
获取信息
监管
会员
获取信息
写入
互助计划资产管理机构

新零售


蚂蚁区块链对新零售能力输出大图
商品溯源
药品安全
食品溯源
跨境物流
供应链金融
高价值生鲜
蚂蚁区块链
区块链
系统服务
存证服务
智能合约服务
跨链互联
共识机制
块链存储
隐私保护
合约引擎
容器服务
阿里云
金融云

7.基础术语

本文将以表格的形式统一对蚂蚁链私有化标准版中涉及的术语进行解释。

本术语表对中文按拼音首字母进行排序。

中文	英文	说明
标识	Identity	在区块链中唯一标识一个账户或者智能合约，长度为 256 位。一般为一个唯一可读内容的哈希值。
存证数据	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，存证数据可以是一个字符串、一个文件的哈希等，以表示文本、文件等存证数据。
根哈希	Root hash	默克尔树的根哈希值，根据当前区块链交易算出。
共识算法	Consensus algorithm	一种分布式系统数据一致性保证的算法，通过一定的协议交互来确保分布式系统的多个参与方达成数据的一致性。常见的算法包括 PBFT、RAFT、POW、POS 等。
共识证明	Consensus proof	用以证明目标数据经过共识算法一致性确认的数据结构。
交易	Transaction	区块链上的一个事务请求，用来承载具体业务操作数据的结构。区块链上所有针对世界状态的变化操作均是基于交易来完成的。
交易个数	Transaction count	某一区块的交易数目。
交易哈希	Transaction hash	交易上链成功后，产生的唯一哈希值。
交易回执	Transaction receipt	是交易的执行结果。区块链是异步的系统，交易执行后需要共识，与传统架构不同，不能直接返回交易执行是否成功，因此需在回执中查看最终交易结果。
交易类型	Transaction type	该交易的类型，如引用存证、内容存证、哈希存证、密文存证、隐私分享、纯密文存证。
交易量汇总	Transactions	交易总量，当前区块链账本上已有保存的交易总数量。
节点信息	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。
可信执行环境	Trusted Execution Environment (TEE)	可信执行环境，提供硬件级别的资源隔离和信任度量功能。近年来在服务器及终端领域，TEE 技术及其应用越发引人关注，其中最具代表性的是 Intel SGX。
联盟	Consortium	不同的机构为了共同合作完成某个业务而结成的联合。
联盟机构	Organization	组成联盟的机构。在 BaaS 平台中，机构指联盟中租户所属的企业。联盟仅支持以租户为单位加入，联盟中不同的租户可能属于同一个机构。
签名证书	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。

区块	Block	区块链上存储打包交易数据以及交易执行结果数据的一种组织形式。区块彼此之间通过前向的应用彼此链接形成区块链。 每个区块记录着上一个区块的哈希值、本区块中的交易集合、本区块的哈希等基础数据。
区块高度	Block height	区块高度，简称块高，用来识别区块在区块链中的位置，并据此找到和这个区块相关的所有基础属性和交易记录。
区块链 ID	Blockchain identification	某一区块链的唯一标识，对应区块链这个底层唯一物理资源。
区块链高度	Blockchain height	当前区块链上出块（Block）的最大数目。
区块链技术	Blockchain	也被称之为分布式账本技术，是一种去中心化的分布式数据库技术，其特点是去中心化、公开透明、不可篡改、可信任。区块链的每笔数据，都会广播全网的区块链节点，每个节点都有全量的、一致的数据。
区块链应用	Application	基于区块链 SDK 开发的应用。
去中心化应用	Decentralized applications（DApp）	与传统中心化应用的主要区别是，DApp 通过客户端直接连接区块链节点，通过智能合约计算和访问数据，没有中心化的后端服务。
燃料	Gas	智能合约在虚拟机中执行计算和存储的消耗度量，通过燃料可防止一些恶意攻击和计算、存储的浪费。
上一块哈希	Previous block hash	当前区块的上一区块哈希。
世界状态	World state	区块链账户的存储状态，包含所有账户的基本存储状态和合约账户的内部存储状态。可以将合约平台理解为一种交易的“状态机”，世界状态描述当前的基本存储状态，经过执行智能合约，世界状态可能发生改变进入另外一个新的世界状态。
数字信封	Digital envelope	数字信封是一种加密技术，通过密码学的方式保证了只有拥有权限的用户才可能解密数字信封中的内容。
私钥	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，即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。
私有交易	Private transaction	与普通交易不同，私有交易不会在公有区块链上进行执行和存储，而是被封装在信封交易的 data 字段中进行发送，最终在私有区块链上进行执行的保存。
信封交易	Envelope transaction	信封交易作为交易的类型，用以封装私有交易。发送信封交易时，私有交易将会被编码后保存在信封交易的 data 字段中。信封交易最终会以存证的形式保存在公有区块链上，但是 data 字段会根据不同需求进行修改。
虚拟机	Virtual machine（VM）	执行智能合约的沙箱环境。
业务 ID	Business identification	业务唯一标识，该区块链应用于哪种业务场景，如溯源、租房等。
业务分类	Category	该交易上链的数据的业务数据格式类型。
业务时间	Business time	该交易的提交生成时间。

账户	Account	区块链上的基本操作对象，一个用户主体在区块链上的逻辑表示。区块链上的所有交易操作均需要基于一个链上已经存在的账户来完成。可分为普通账户和合约账户。
证书颁发机构	Certificate Authority（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。
证书申请	Certificate request	证书签名请求文件（Certificate Signing Request，CSR），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，即该 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。
智能合约	Smart Contract	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。一个智能合约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。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。