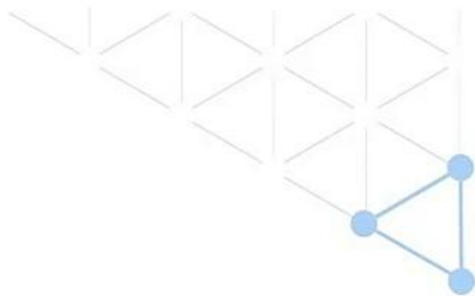


蚂蚁链智能合约简介

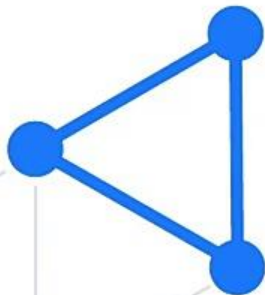
- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程 目标

- 了解蚂蚁链
- 了解蚂蚁链智能合约平台
- 了解蚂蚁链基础术语介绍



01 蚂蚁区块链



蚂蚁链简介

蚂蚁链

- 由蚂蚁集团开发（ANTCHAIN）
- 技术服务
 - BaaS平台
 - 开放联盟链
 - 应用快速搭建平台
 - 区块链融资租赁
- 技术优势
 - 共识机制
 - 智能合约
 - 可信计算
 - 隐私保护
 - 跨链交互



蚂蚁区块链

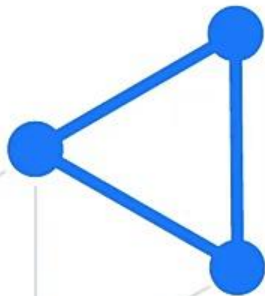
蚂蚁链简介

应用场景

- 金融、保险行业
 - 跨境汇款
 - 相护宝
- 融资租赁
- 区块链合同
- 溯源
 - 慈善公益善款溯源
 - 正品溯源
- 政务民生
- 数字物流
- 医疗健康



02 蚂蚁智能合约平台简介



开放联盟链

- 类公链设计（公有制许可）
 - 公有链（人人可参与，但承载能力弱）
 - 联盟链（注册或邀请会员制，承载能力强）
 - 私有链（仅限个人或公司内部使用）
- 多种智能合约模板
- 超强性能
- Cloud IDE
- 个人用户开通送1亿Gas

	公有链	联盟链	私有链
参与者	任何人	联盟成员（注册会员）	个体或公司内部
记录者	所有参与者	联盟成员	个体或公司内部成员
中心化程度	完全去中心化	联盟内去中心化	公司内去中心化
突出特点	信用的自建立	效率和成本优化	透明和可追溯
承载能力	弱，约几十-几百笔/秒	极高，万-千万笔/秒	极高，十万-千万笔/秒

蚂蚁智能合约平台

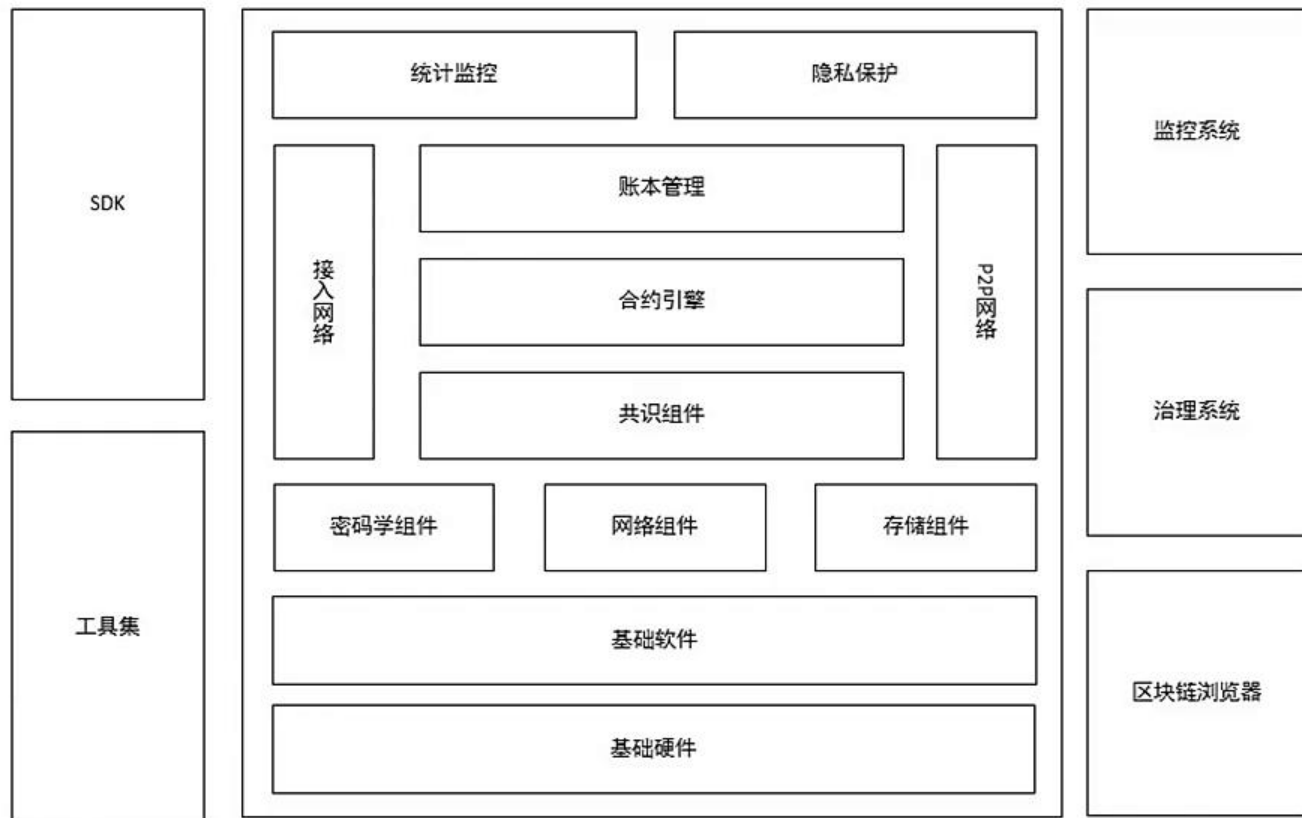
蚂蚁区块链合约平台通过引入 P2P 网络、共识算法、虚拟机、智能合约、密码学、数据存储等技术特性，构建一个稳定、高效、安全的图灵完备智能合约执行环境，提供账户的基本操作以及面向智能合约的功能调用。基于合约平台提供的能力和功能特性，应用开发者能够完成基本的账户创建、合约调用、结果查询、事件监听等。

功能特性

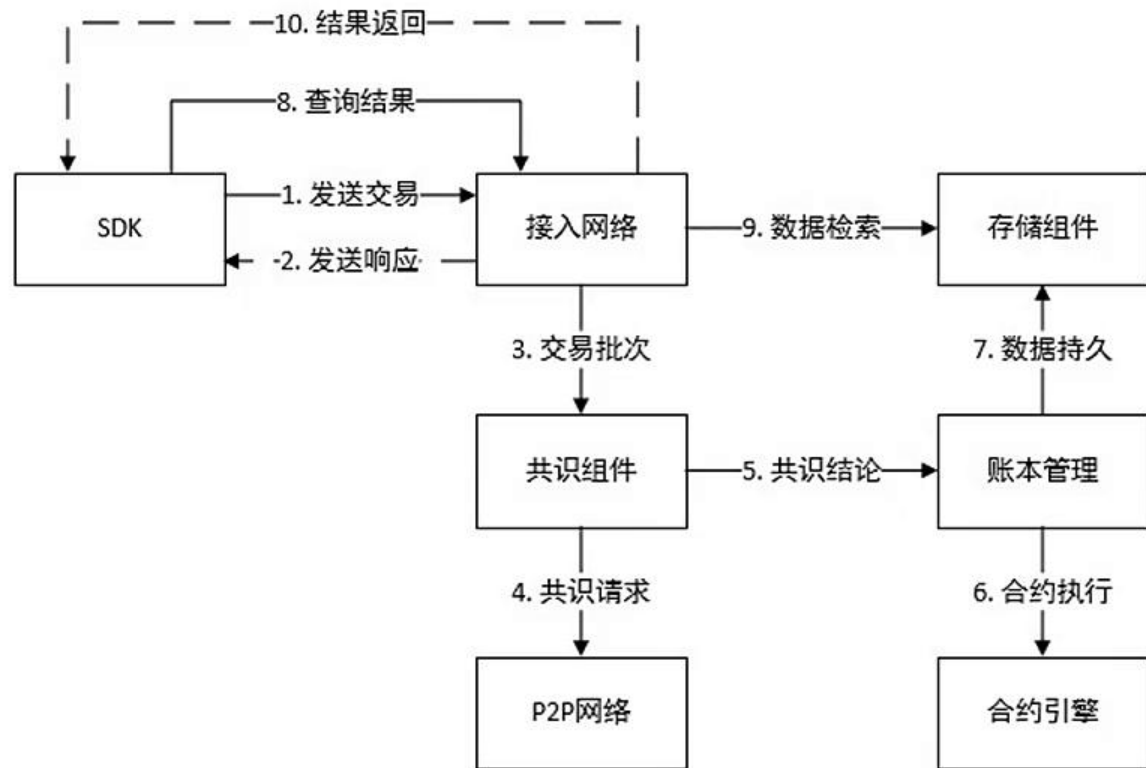
- 账户操作
- 合约体系
 - EVM引擎
 - WASM引擎
- 区块查询
- 事件监听
- 数据隔离
- 隐私保护
- SPV验证



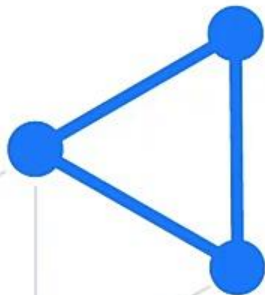
蚂蚁智能合约平台-系统架构



蚂蚁智能合约平台-核心逻辑



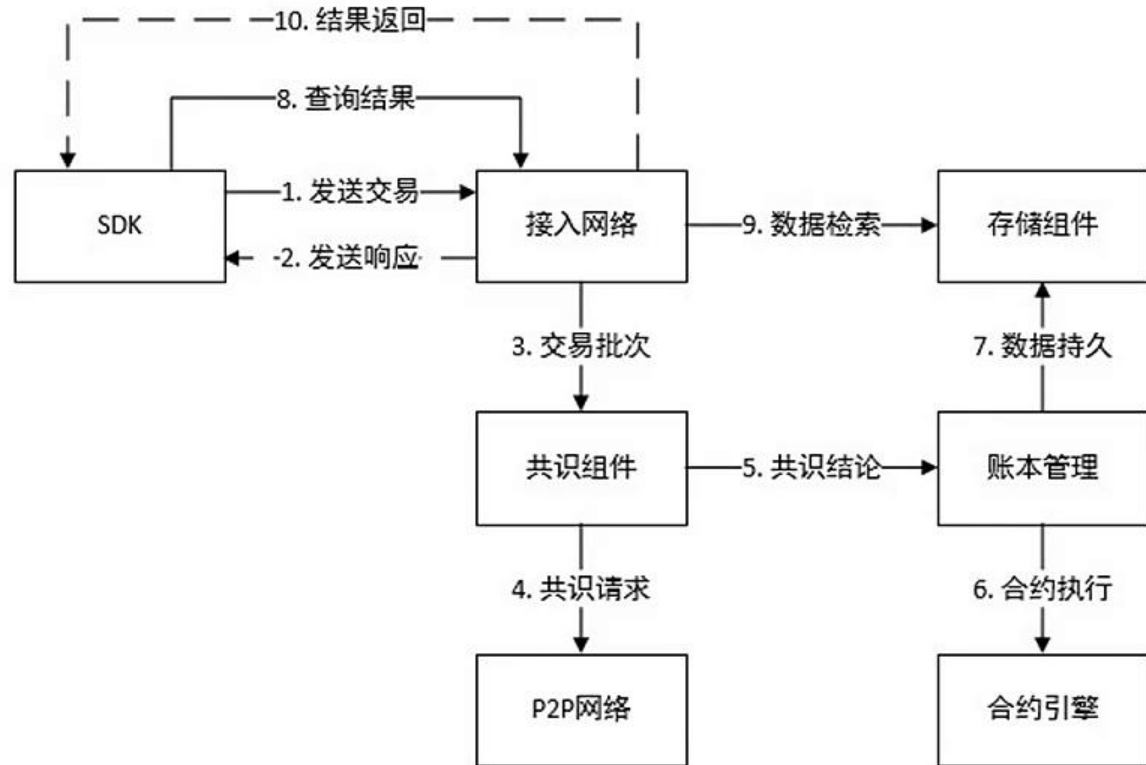
03 蚂蚁链基础术语介绍



蚂蚁链基础术语介绍

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。
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。
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。
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。
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。
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。

蚂蚁智能合约平台-核心逻辑



谢谢