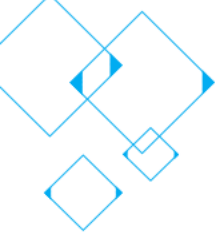


第1章 FISCO BCOS区块链概述



CONTENTS

目录

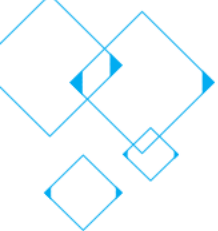
第一章 认识联盟链

第二章 FISCO BCOS架构解读

第三章 FISCO BCOS特性分析

第四章 FISCO BCOS应用案例





第一章 认识联盟链

1.1 什么是区块链

1.2 什么是联盟链

1.3 联盟链的特点

1.4 国内常见的联盟链平台

1.5 FISCO BCOS联盟链介绍

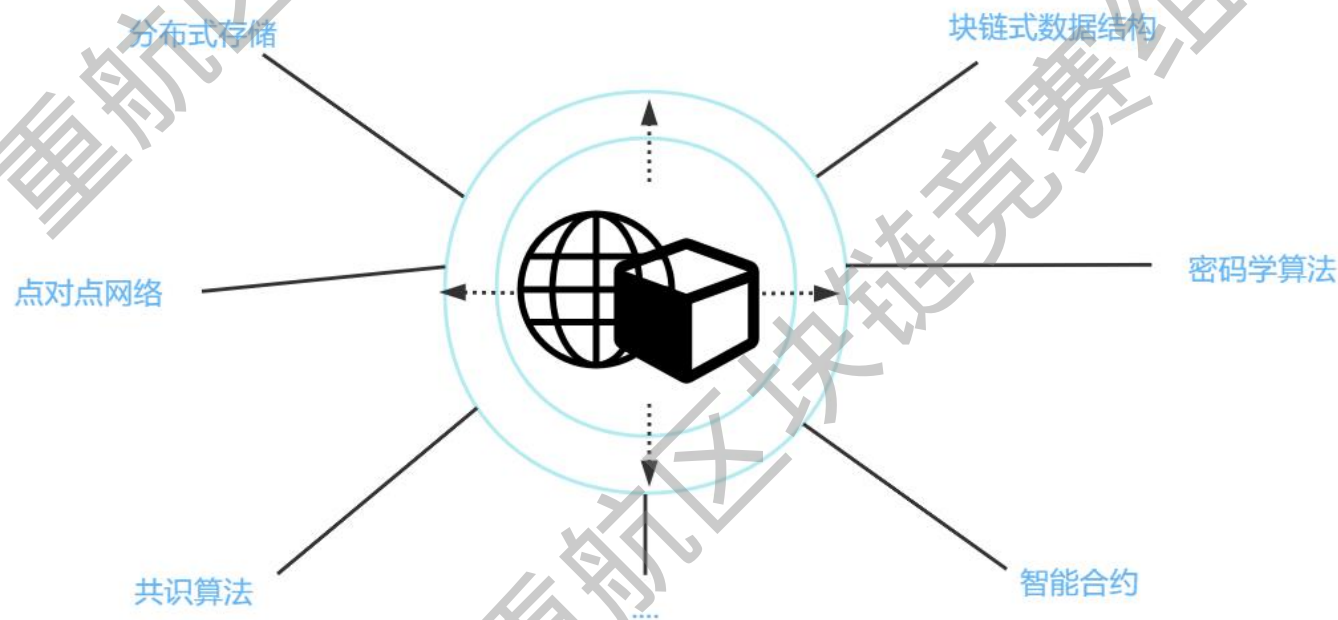
章节

CONTENTS



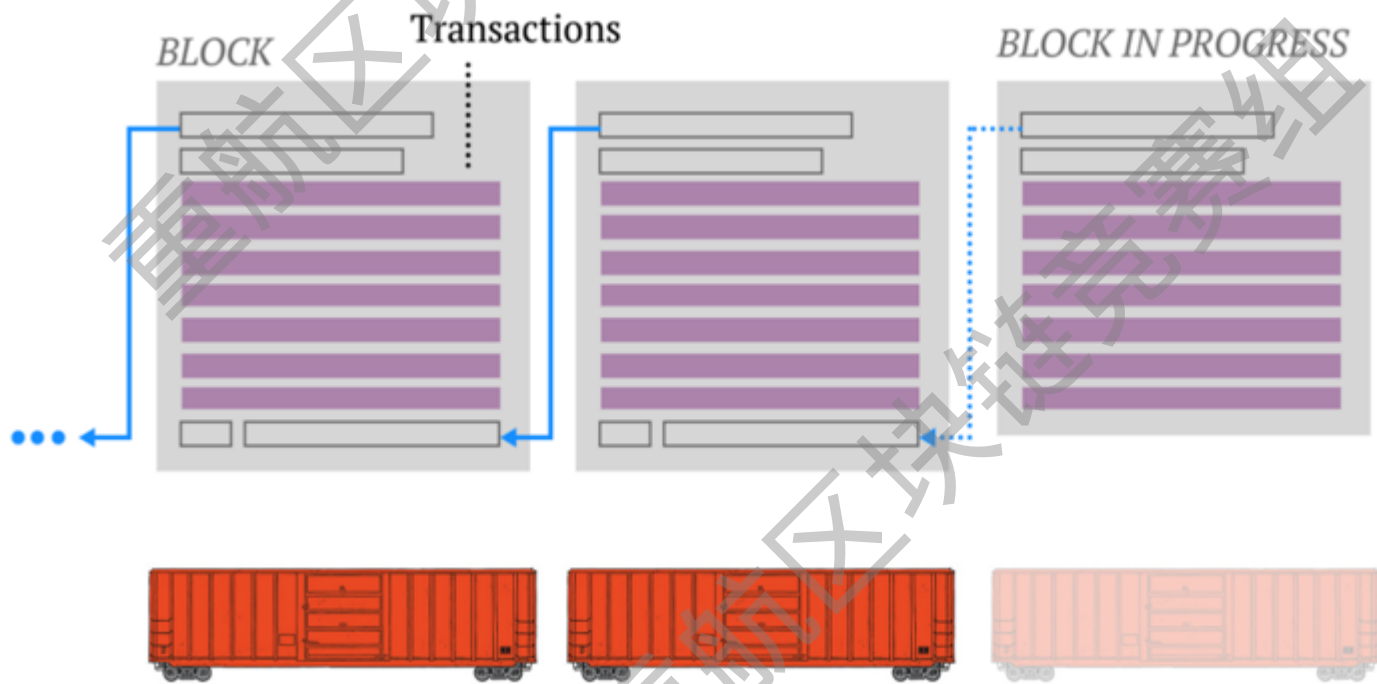
什么是区块链？

- 区块链是比特币出现后提出的一个概念，从技术架构上讲，区块链是由分布式架构与分布式存储、块链式数据结构、点对点网络、共识算法、密码学算法、博弈论、智能合约等多种信息技术共同组成的整体解决方案。



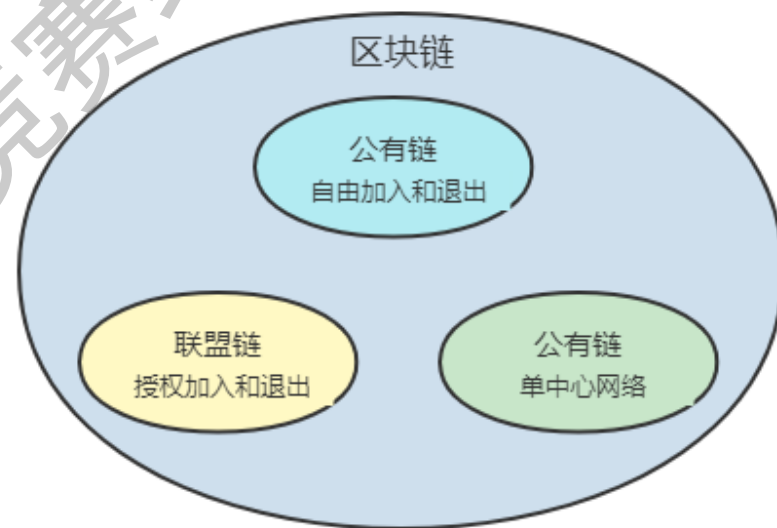
什么是区块链？

- 从数据结构上来讲，区块链以“块”的形式收集信息，一旦块被数据填充，就会被链接到前一个区块上，这使得数据按时间顺序链接在一起。类比于火车，火车的每一节车厢就是一个“区块”。



什么是联盟链?

- 联盟链属于区块链的一种，一般是指由多个主体达成一定的协议，或建立了一个业务联盟后，多方共同组建的链。**联盟链仅对联盟成员开放全部或部分功能，联盟链上的读写权限、以及记账规则都按联盟规则来“私人定制”，实现“部分去中心化”功能。**
- 除了联盟链外，区块链还被细分为公有链和私有链。
 - 公有链：指任何人都可以参与的链。
 - 私有链：只对单位或个人开放的区块链。



联盟链的特点

● 联盟链与公有链、私有链的比较

	公有链	联盟链	私有链
准入限制	自由加入和退出	授权加入和退出	链所有者
读写权限	任何人	关联用户	仅限受邀用户
记账权限	所有参与者	联盟协商确定	链所有者
中心化程度	去中心化	弱中心化	强中心化
激励机制	需要	可选	无
交易速度	慢	快	快
使用场景	加密货币	供应链金融、银行、物流、电商等	机构/公司/个人

国内常见的联盟链平台

- 国内常见的联盟链平台

- 中国区块链研究联盟（CBRA）
- 中国分布式总账基础协议联盟（ChinaLedger）
- 区块链服务网络（BSN）
- R3社区联盟
- 超级账本（Hyperledger）
- 金链盟（FISCO BCOS）

FISCO BCOS联盟链介绍

- FISCO BCOS联盟链背景

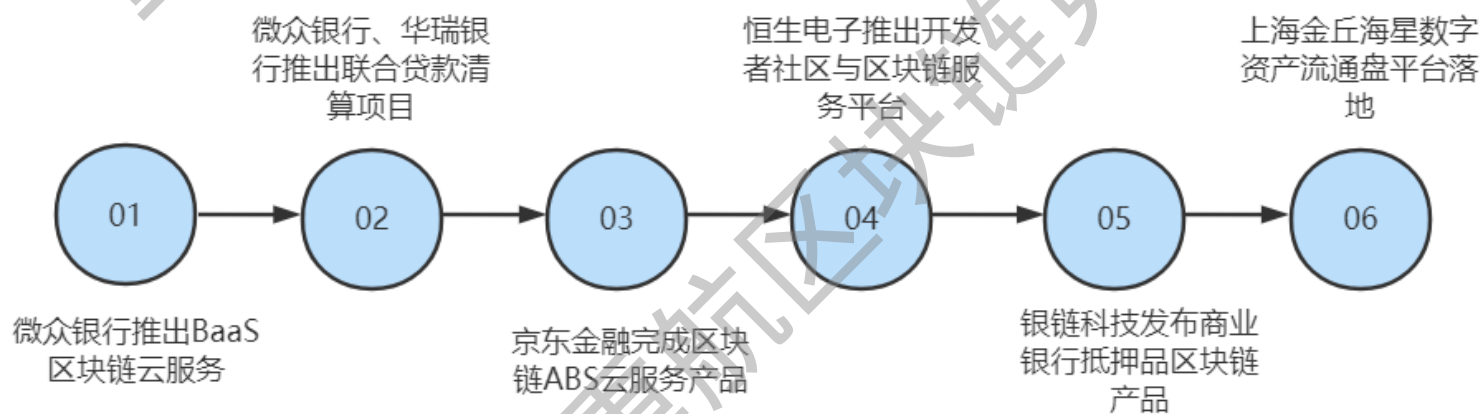
- FISCO BCOS是一款**开源**的企业级金融联盟链的底层平台，由金融区块链合作联盟（简称：金链盟）开源工作组打造，并于2017年正式对外开源。



FISCO BCOS联盟链介绍

● FISCO BCOS联盟链发展

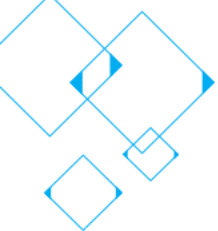
- 截止2019年6月，FISCO BCOS 开源生态圈已涵括2000多家企业机构、逾40000名社区成员，并且仍在与日俱增中。基于 FISCO BCOS 搭建的应用有数百个，其中超120个应用已在生产环境中稳定运行，场景覆盖**政务、金融、公益、医疗、教育、交通、版权、商品溯源、供应链、招聘、农业、社交、游戏**等多个领域，并且涌现出**粤港澳健康码互认系统、人民网人民版权平台、中国澳门智慧城市建设**等重磅应用。



FISCO BCOS联盟链介绍

- FISCO BCOS联盟链特色与优势

- FISCO BCOS 采用联盟链的技术架构，以满足分布式商业场景中合法合规地进行多方对等协作为目标，兼顾金融创新与金融稳定，融汇吸收了分布式架构、分布式存储、点对点网络协议、加密算法、共识算法、智能合约以及虚拟机等多类技术。具备高性能、安全可控、功能丰富等优势，为开展区块链应用提供可靠的基础设施。



第二章 FISCO BCOS架构解读

1.1 FISCO BCOS整体架构

1.2 群组架构

1.3 并行计算

1.4 分布式存储

1.5 多引擎

1.6 分布式算法

章节

CONTENTS



FISCO BCOS整体架构

- FISCO BCOS 2.0版本中，提出了“**一体两翼多引擎**”的构架，将系统的吞吐量进行横向扩展，性能、安全性、易用性都得到了大幅提升。其含义如下：

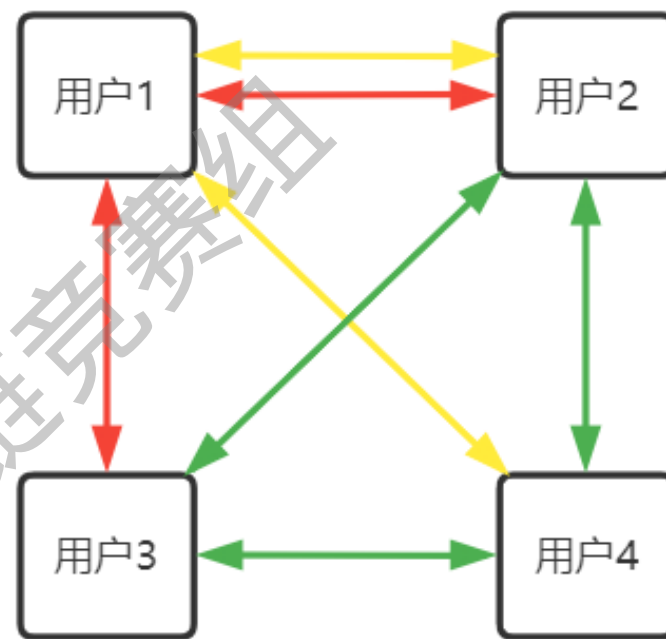
- 一体：群组架构
- 两翼：并行计算和分布式存储
- 多引擎：CRUD、预编译合约、控制台、平台服务、业务模版、虚拟机等功能



群组架构

- 群组架构能够帮助企业快速组建联盟和建链。企业可以根据业务场景和关系不同，建立不同的群组和不同的账本，多个账本之间的数据可以进行共享和共识，从而快速丰富业务场景，简化企业对联盟链的部署和运维成本。为方便理解，可类比微信群聊，几个人就可以快速拉个主题群进行交流。同一个人可以参与到自己感兴趣的多个群里，并行地收发信息。现有的群也可以继续增加成员。

群组1: 
群组2: 
群组3: 



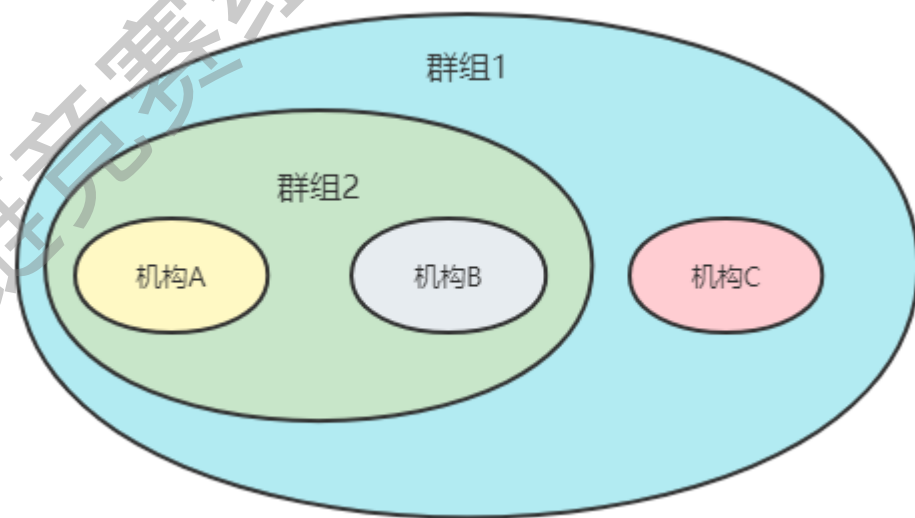
群组架构

- 场景理解

- 机构A、B、C构成一个区块链网络，共同运行业务1；一段时间后，机构A、B启动业务2，并且不希望该业务被机构C感知，如何解决？

- FISCO BCOS2.0 解决方案

- 让机构A和机构B新建一个群组运行业务2即可。



群组架构

● 群组架构的优势

- 具有**隐私保护**，各群组之间相互独立，各自维护自己的交易数据和事务；
- 运维管理员只需要维护一条链，**减少运维成本**；
- 群组能够快速帮助企业搭建业务，**灵活扩展业务范围**；
- 在跨群组之间的消息互通，则会带上验证信息，是**可信和可追溯**的。

并行计算

- 并行计算模型

- 在区块链的世界中，交易是组成事务的基本单元。而**TPS**（Transaction per Second，每秒交易量）是交易吞吐量的性能评估指标，TPS越高，性能越高。FISCO BCOS2.0中设计了一种**基于DAG（有向无环图）的并行交易执行器**（PTE，Parallel Transaction Executor），让区块链中的交易尽可能地并行执行。**计算机核数越多，性能就越高。**

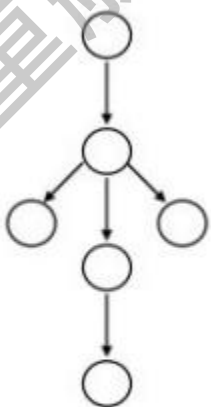
并行计算

- 什么是有向无环图？

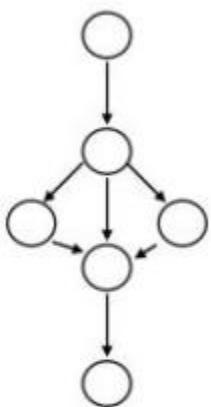
- DAG是一种数据结构，同链表和树不一样，它是可以有闭合的Graph图，且一个节点到另一个节点是单向的，图中不允许出现一个节点出发后能回到起点的情况。



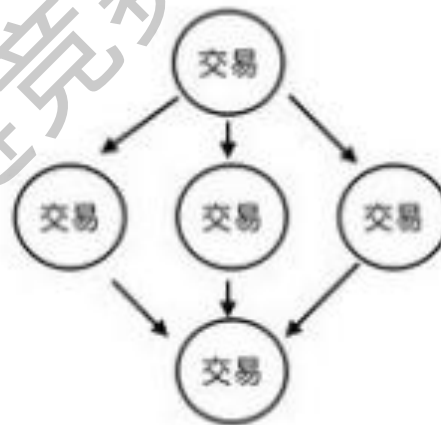
链表



树

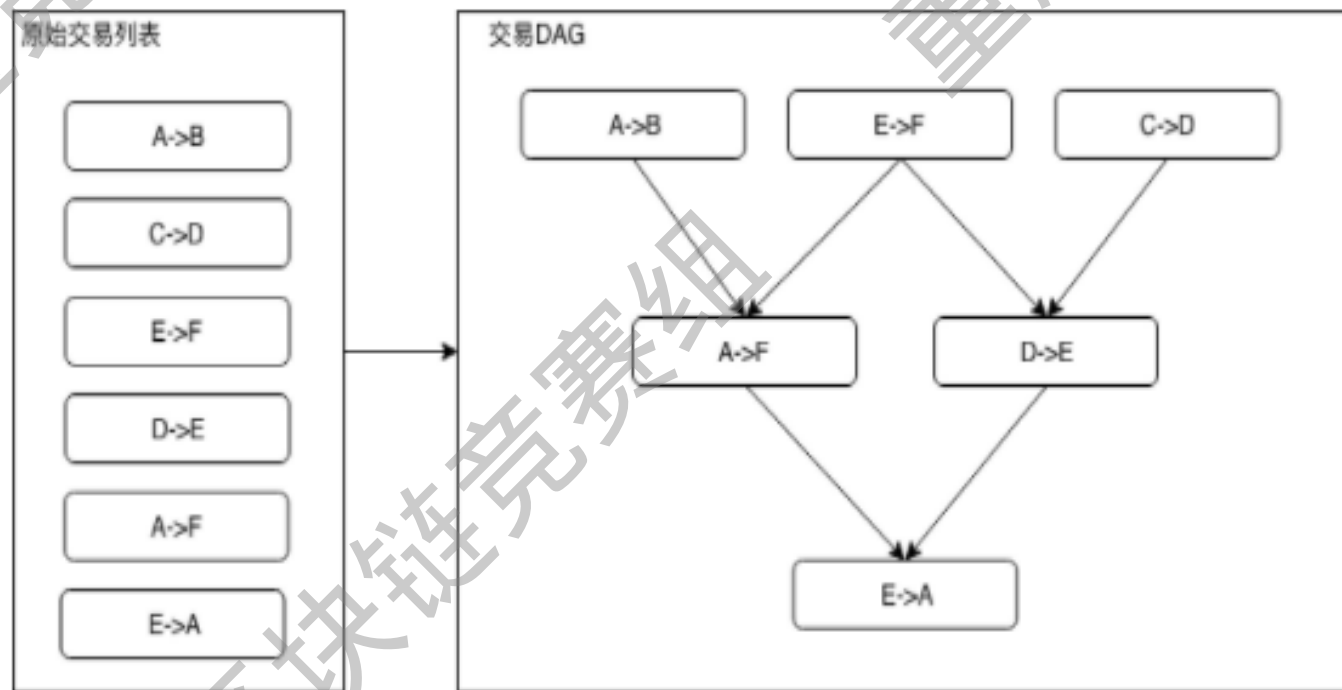


图



并行计算

- 在一批交易中，可以通过一定的方法识别每笔交易需要占用的互斥资源，再根据区块中的交易顺序及互斥资源构造一个交易依赖DAG图，凡是入度为0（无依赖的前序任务）的交易可以并行执行。



并行计算

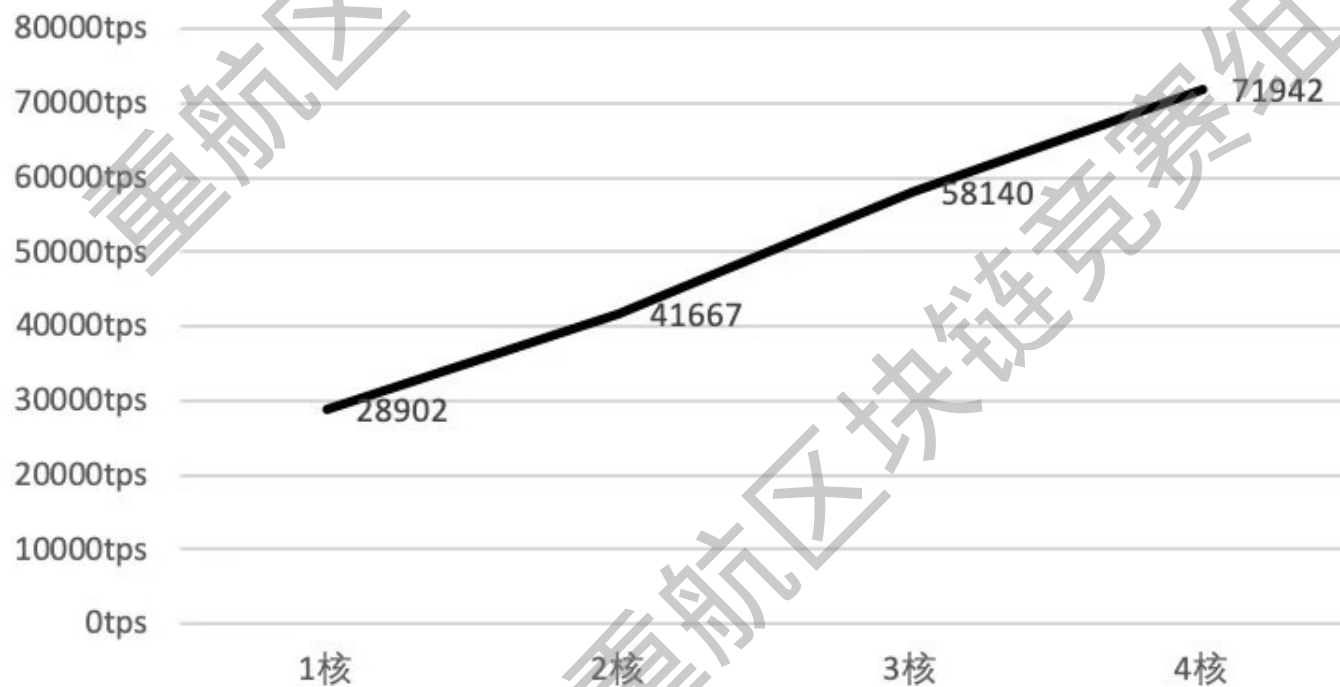
- PTE（并行）和Serial（串行）性能对比



并行计算

● PTE可扩展性

- 随着核数增加，PTE的交易吞吐量呈近似线性递增
- 随着核数在增加，性能增长的幅度在放缓



分布式存储

- 分布式存储

- FISCO BCOS 1.0中，节点采用MPT数据结构，通过LevelDB将数据存储于本地，这种模式受限于本地磁盘大小，当业务量增大时数据会急剧膨胀，要进行数据迁移也非常复杂，给数据存储带来较大的成本和维护难度。
- 在FISCO BCOS 2.0中，通过对底层存储的重新设计，实现了AMDB（分布式存储），使用不同于MPT的方式来实现追溯，带来了性能上的提升。

分布式存储

● 世界状态

- 智能合约执行过程产生的状态数据，经过共识机制确认，分布式的保存在各节点上，数据全局一致，可验证难篡改，所以称为“**世界状态**”。
- 世界状态可进一步分为 MPTStates 和 StorageStates:
 - ✓ **MPTStates:** 使用**MPT** 树存储账户的状态，与以太坊一致；
 - ✓ **StorageState:** 使用分布式存储的表结构存储账户状态，不存历史信息，去掉了**对 MPT 树的依赖**，性能更高。

分布式存储

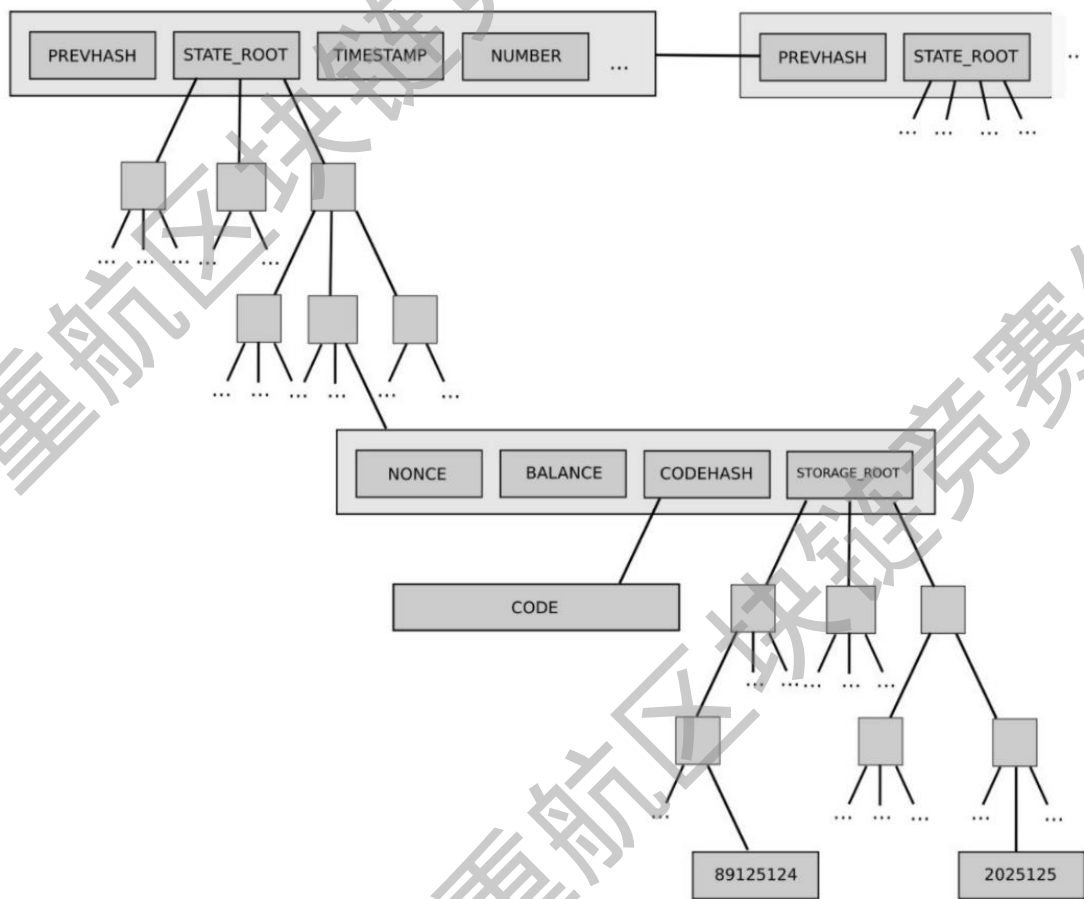
● MPT存储

- MPT（Merkle Patricia Trie，默克尔前缀树）是一种数据存储结构，状态数据由账号组成，包括Nonce、Balance、CodeHash 和 StorageRoot，账号在 MPT 里是一个叶子节点，当任意一个账号字段发生变化时，该账号所在的叶子的 Hash 值也会发生变化，从而影响到顶部的StateRoot。

MPT 追求极致的可证明性和可追溯性的同时带来了大量的 Hash 计算，打散了底层数据存储的连续性，也因此性能方面做出了妥协。

分布式存储

● MPT存储结构



分布式存储

- AMDB（分布式存储）

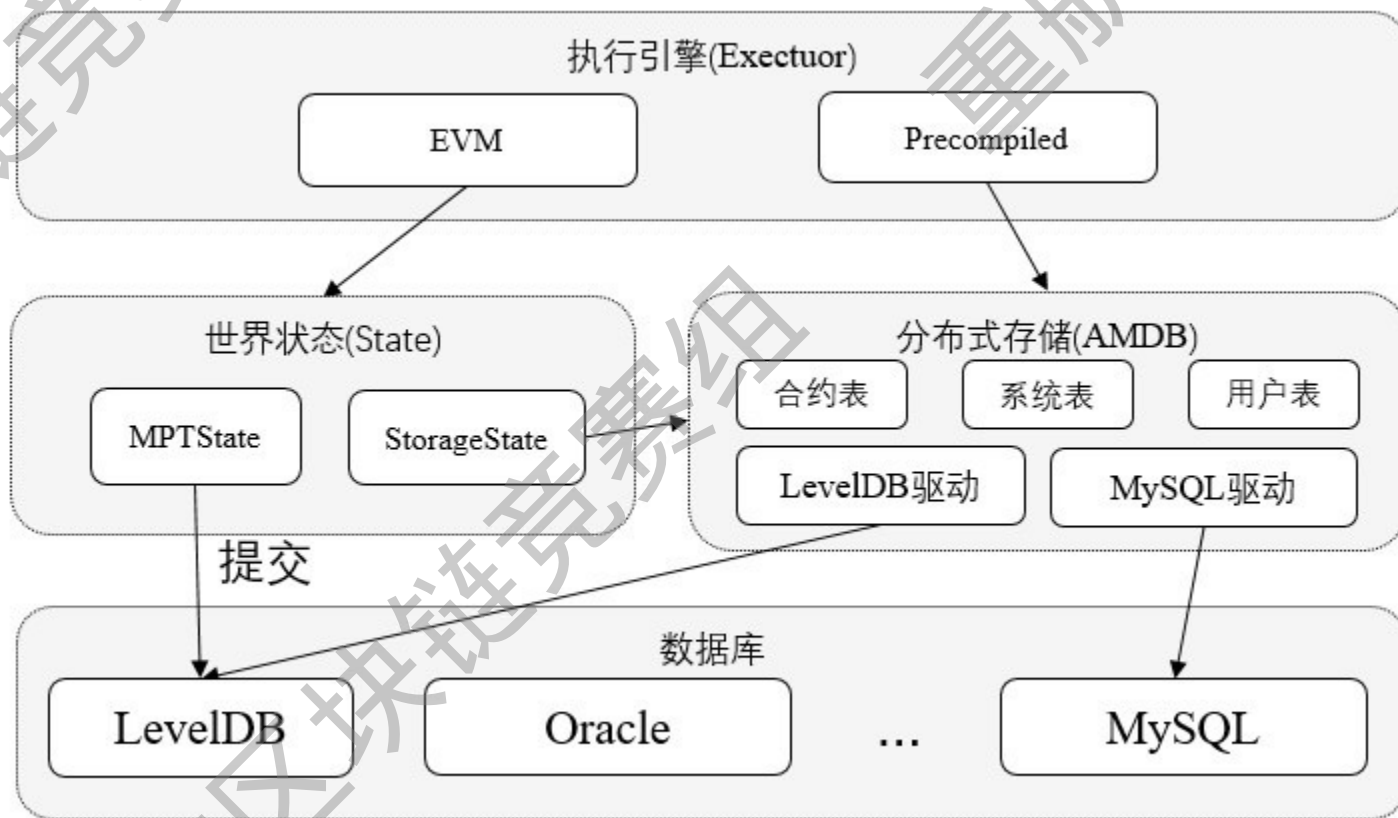
- 分布式存储重新抽象了区块链的底层存储模型，实现了类 SQL 的抽象存储接口，支持多种后端数据库，包括 KV 数据库和关系型数据库。引入了分布式存储后，数据读写请求不经过 MPT，直接访问存储，结合缓存机制，存储性能相比基于 MPT 的存储有大幅提升。

	StorageState	MPTState
存储方式	AMDB存储	MPT存储
历史状态查询	不支持	支持
存储性能	高	低

分布式存储

● FISCO BCOS存储架构

- FISCO BCOS在继承以太坊MPT存储的同时还引入了分布式存储。
- 当使用MPTState时，合约局部变量保存在MPT树中。
- 当使用StorageState时，合约局部变量保存在AMDB表中。

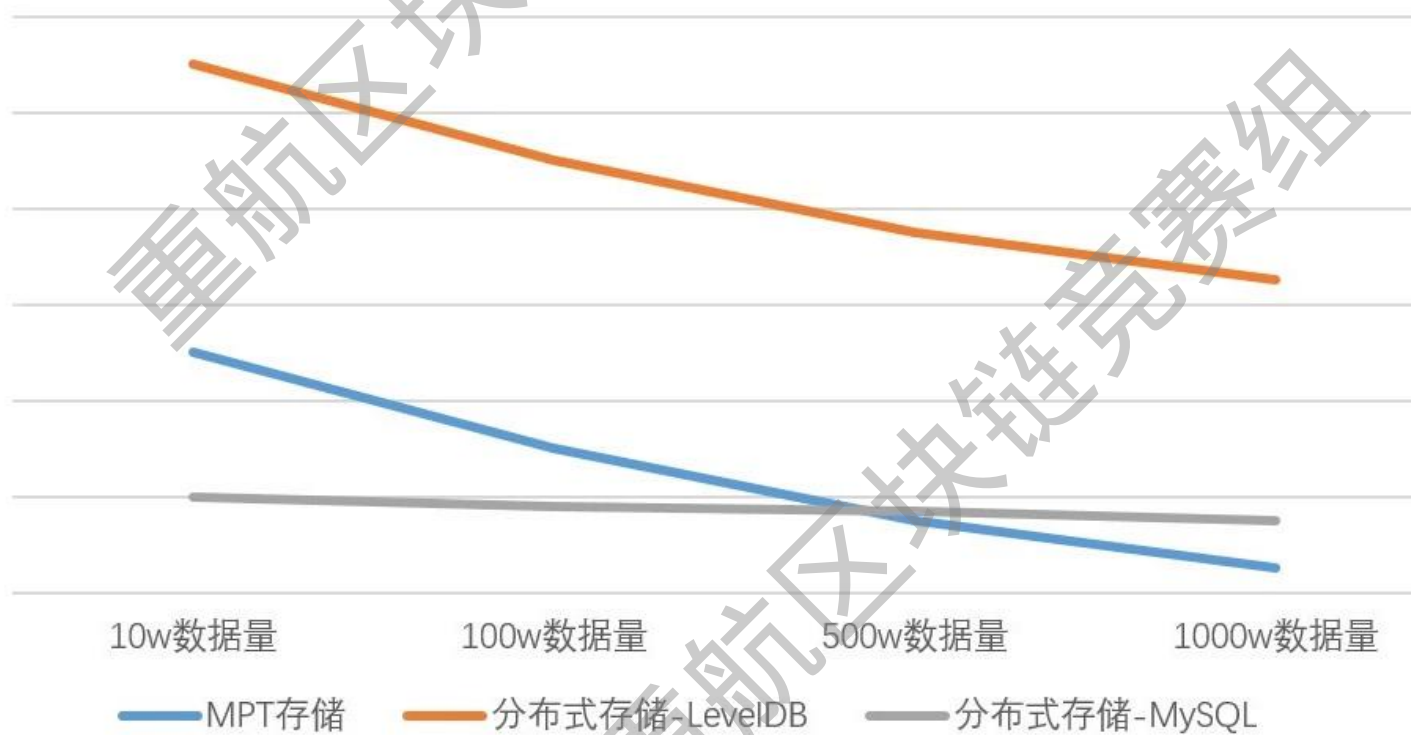


分布式存储

● 分布式存储与MPT存储性能对比

存储模型性能对比

腾讯云、8核CPU、16G内存、SSD本地磁盘、MariaDB 5.5.60



分布式存储

● FISCO BCOS 分布式存储优势

- 支持多种存储引擎，选用高可用的分布式存储系统，可以支持数据简便快速地扩容；
- 将计算和数据隔离，节点故障不会导致数据异常；
- 数据在远端存储，数据可以在更安全的隔离区存储，这在很多场景中非常有意义；
- 世界状态的存储从原来的 MPT 存储结构转为分布式存储，避免了世界状态急剧膨胀导致性能下降的问题；
- 优化了数据存储的结构，更节约存储空间。

多引擎

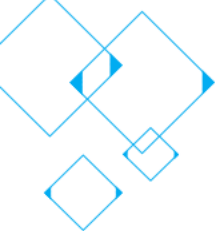
- 多引擎包含了预编译合约、CRUD 合约、控制台、虚拟机等一系列功能特性。
 - **预编译合约**：提供预编译合约框架，支持C++编写合约，使合约调用响应更快，消耗更少，更易于并行计算，提升系统效率。
 - **CRUD合约**：基于预编译合约实现，提供面向SQL编程的区块链应用开发，数据分布式存储，效率更高。
 - **控制台**：拥有丰富的命令和良好的交互体验，帮助用户开发、运维、管理区块链系统。
 - **虚拟机**：引入最新的以太坊虚拟机版本，同时，引入了EVMC扩展框架，支持扩展不同虚拟机引擎。

- FISCO BCOS中的共识算法

- FISCO BCOS基于多群组架构实现了插件化的共识算法，不同群组可运行不同的共识算法，组与组之间的共识过程互不影响，FISCO BCOS目前支持PBFT(Practical Byzantine Fault Tolerance)和Raft(Replication and Fault Tolerant)两种共识算法。

- ✓ **PBFT共识算法：**拜占庭容错类算法，可容忍不超过三分之一的故障节点和作恶节点，可达到最终一致性；

- ✓ **Raft共识算法：**普通容错类算法，可容忍一半故障节点，不能防止节点作恶，可达到一致性。



CONTENTS

章节

第二章 FISCO BCOS特性分析

1.1 性能指标

1.2 安全方案

1.3 运维治理

1.4 开发支持



性能指标

- 区块链的性能指标最常见的主要是TPS（Transaction Per Second），交易延迟等。
 - TPS：每秒能处理和确认的交易数量
 - 交易延迟：交易发送到区块链网络后，经过验证、计算和共识一系列流程后，最终确认的时间。

FISCO BCOS系统性能（PBFT共识，单链）	
TPS	2万+（PBFT）
交易延迟	秒级

安全方案

- 区块链的安全性主要体现在系统层面和业务层面，系统层面主要有网络攻击、系统渗透、数据破坏和泄露等问题；业务层面主要有越权操作、逻辑错误、隐私保护等问题。

FISCO BCOS 安全解决方案	
准入机制	PKI身份认证
隐私保护	支持群签名、环签名、同态加密
证书管理	支持证书颁发、撤销、更新
物理隔离	群组间数据隔离
权限控制	支持细粒度权限控制

运维治理

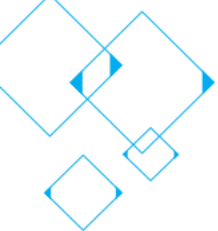
- 系统运行过程中，可通过监控系统对各种运行指标进行监控，如CPU/内存占比、区块高度、交易数量等，以便对系统的健康程度进行评估，当出现故障时发出告警通知，便于运维快速反应，进行处理。

FISCO BCOS 运维治理	
区块链浏览器	支持
可视化节点管理	WeBASE中间件
动态节点管理	支持节点动态新增、剔除、变更
监控管理	输出统计日志，WeBASE提供监控工具
审计管理	WeBASE提供审计入口

开发支持

- 构建一个区块链系统往往是繁琐和复杂的，FISCO BCOS提供了一键部署的脚本工具，简化了链的部署流程和配置修改，帮助开发者快速搭建开发调试环境；另外FISCO BCOS提供了供多种语言调用的SDK，帮助开发者根据自身业务要求，开发应用程序。

FISCO BCOS开发支持	
合约开发工具	WeBASE-IDE
开发部署工具	一键搭建链脚本工具
区块链交互工具	控制台
SDK	多SDK支持，包括Java、go、python等



第二章 FISCO BCOS应用案例

章节

1.1 物流保险平台

1.2 产品溯源

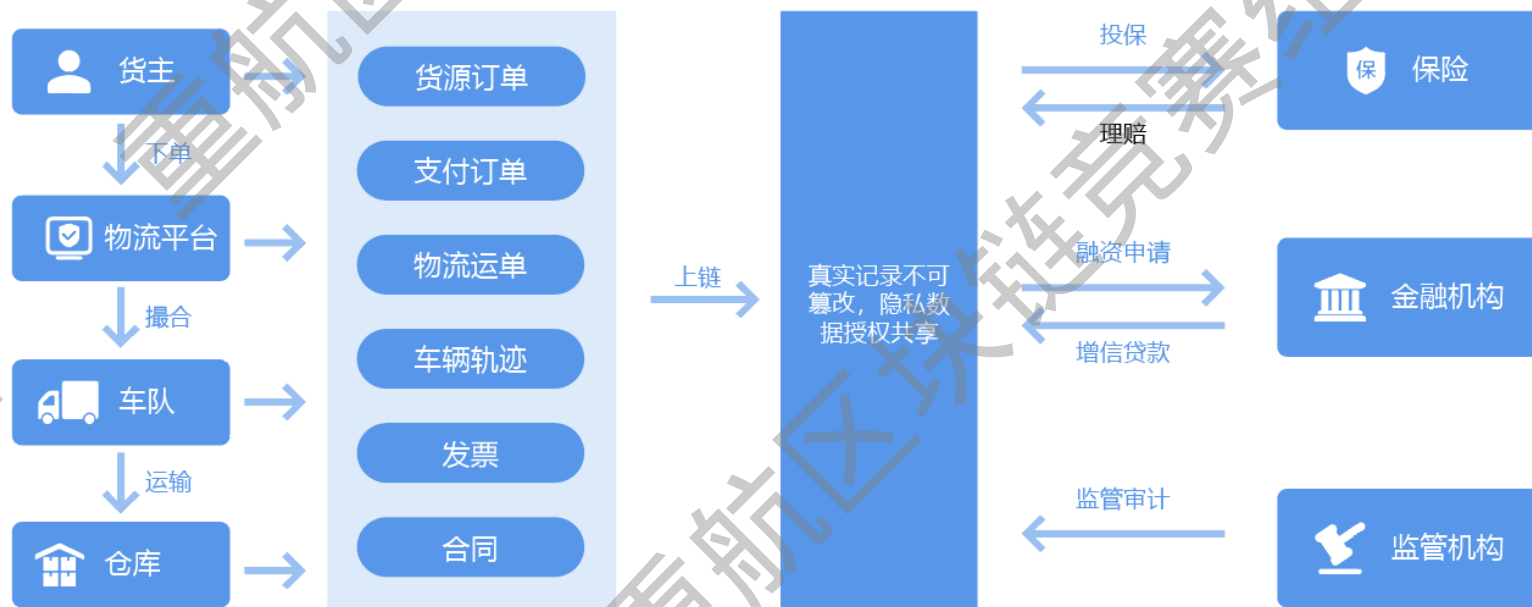
1.3 文化版权

1.4 应用场景



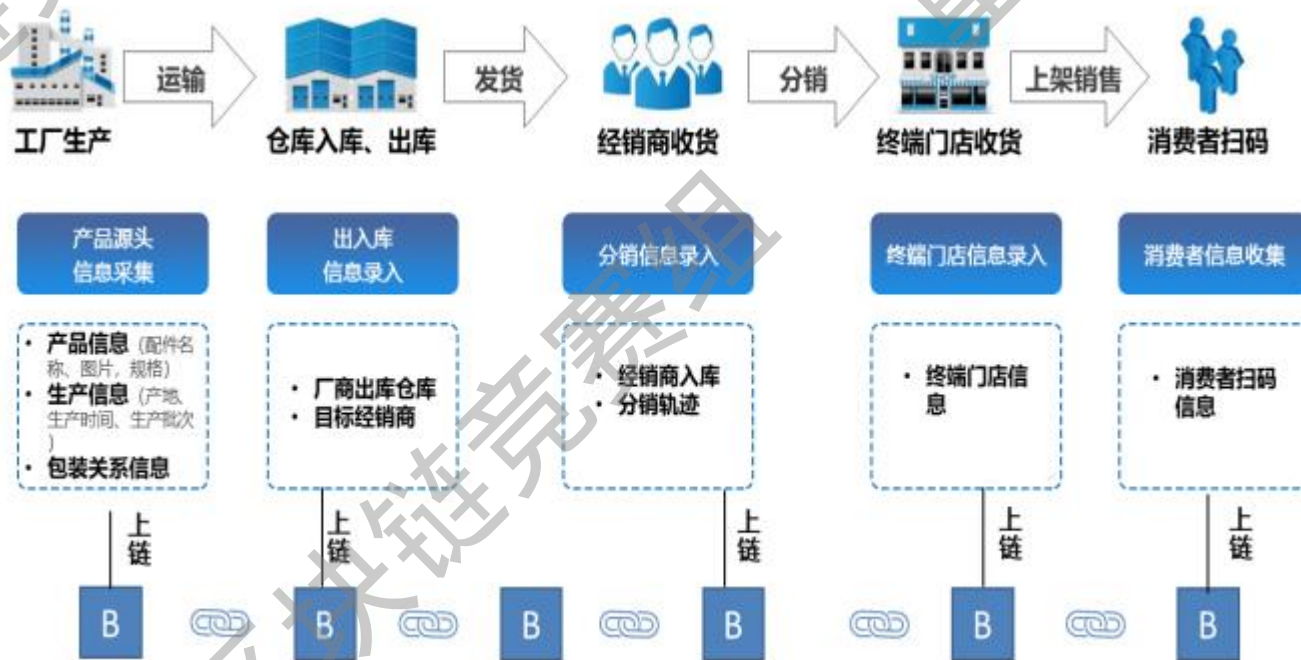
物流保险平台

- 融合大数据和人工智能技术为司机、物流公司、货主的真实情况提供有力的第三方佐证，提升金融、保险机构对平台中需要融资或投保主体的风控能力；同时降低物流金融的信用成本，降本提速。



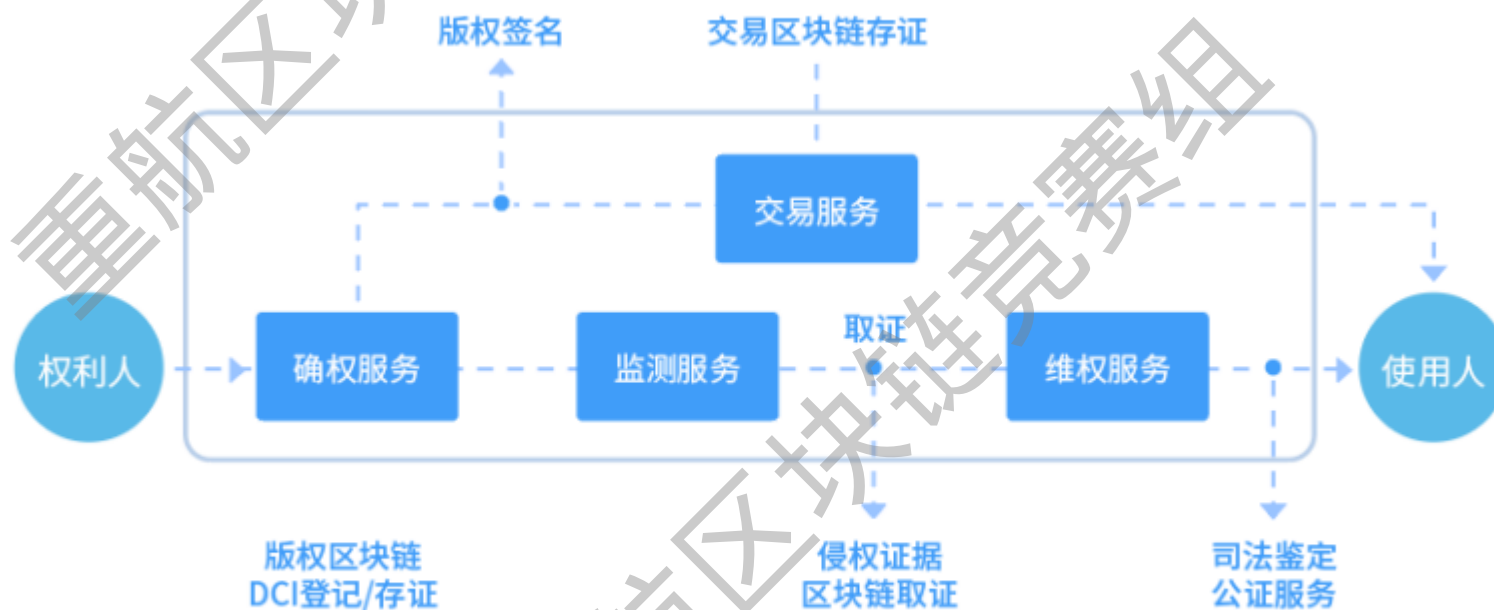
产品溯源

- 通过对产品的生产、流通、营销等环节的信息实时上链，实现一物对一码的全流程正品溯源，建立品牌商和消费者之间的信任桥梁，提升企业品牌价值。



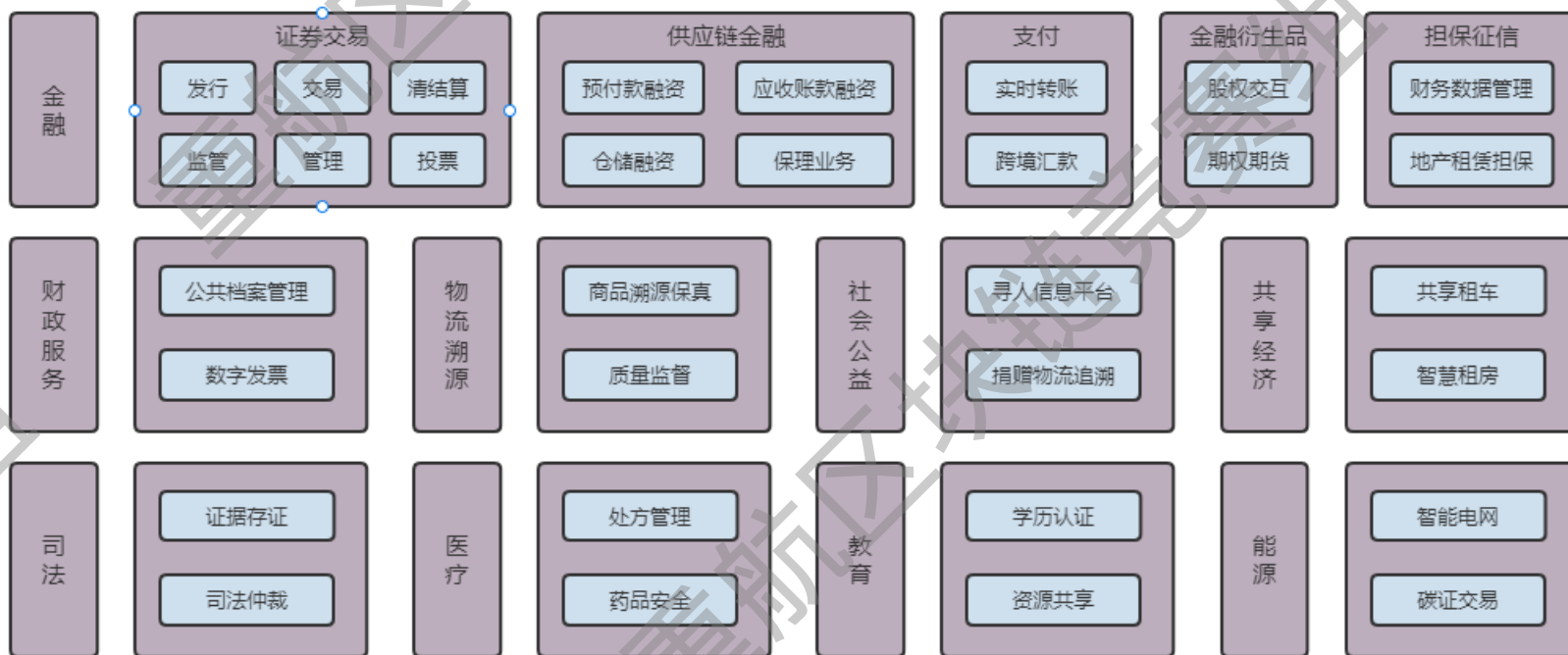
文化版权

- 解决版权内容权属、分发和获利分成问题，让正版作品的交易结合智能合约上链；使用大数据发现和辨别侵权行为，使用区块链为维权提供侵权依据。



应用场景

- 依托于区块链的不可篡改、可追溯等特性，区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域，展望未来，区块链技术将会在未来发挥更大的潜能，创造更大的价值！



作业

1. 什么是联盟链？
2. 联盟链与公有链的区别有哪些？
3. 说出常见两个联盟链？
4. FISCO BCOS2.0的整体架构是什么？
5. 如何理解群组架构？优势是什么？
6. FISCO BCOS2.0中是如何提高计算效率的？TPS如何？
7. 说一说MPT存储和AMDB存储的不同？AMDB有何优势？
8. FISCO BCOS2.0采用了哪些安全解决方案？
9. FISCO BCOS还可以应用在哪些领域？

课程总结

- 本课程详细介绍了
 - 联盟链的概念及公有链、私有链和联盟链的特点
 - FISCO BCOS联盟链背景及发展
 - FISCO BCOS区块链的系统架构及优势
 - FISCO BCOS区块链的系统特性
 - FISCO BCOS可能的应用场景

谢谢