第 3 章

FISCO BCOS 概述

3.1 FISCO BCOS 简介


1min

3.1.1 起源与背景

FISCO BCOS 是由深圳市金融区块链发展促进会(以下简称“金链盟”)开源工作组牵头研发的金融级、国产安全可控的区块链底层平台。作为最早开源的国产联盟链底层平台之一,FISCO BCOS 于 2017 年面向全球开源。

FISCO BCOS 持续攻关关键核心技术,单链性能突破 10 万 TPS。首创 DMC 算法大幅度提升性能,推出 3 种架构形态以灵活适配业务需求;全链路国产化,采用国密算法与软硬件体系,支持国产操作系统,适配国产芯片和服务器,支持多语言多终端国密接入。拥有覆盖底层、中间件、应用组件的丰富周边组件。

底层平台可用性已经被广泛地应用于实践检验,支撑政务、金融、医疗、“双碳”、跨境数据流通等关乎国计民生的重点领域,已落地超过 400 个标杆应用,在助力实体经济发展、促进公平与可持续等方面贡献力量。

社区以开源链接多方,截至 2023 年 12 月,围绕 FISCO BCOS 构建的国产开源联盟链生态圈已汇聚了超过 5000 家机构、超 10 万名个人成员,以及 50 家认证合作伙伴、500 余名核心贡献者。社区认证了 63 位 FISCO BCOS MVP,发展了 12 个专项兴趣小组 SIG,此外与上百所知名院校开展人才共育合作,培育区块链产业人才超 8 万人,已发展成为最大最活跃的国产开源联盟链生态圈之一。


2min

3.1.2 关键特性

1. 三种架构形态

FISCO BCOS v3.0 采用微服务架构,但同时也支持灵活拆分组合微服务模块,从而构建不同形态的服务模式,包括轻便 Air 版本、专业 Pro 版和大容量 Max 版。

(1) 轻便 Air 版:拥有与 v2.0 版本相同的形态,所有功能在一个区块链节点中(all-in-one)。该架构简单,可快速部署在任意环境中。可以用它进行区块链入门、开发、测试、POC 验证等工作。

(2) 专业 Pro 版:该架构通过将区块链节点的接入层模块独立为进程,在实现接入层与核心模块分区部署的同时,让区块链核心功能模块以多群组方式扩展。该架构实现了分

区隔离，可应对将来可能的业务拓展，适合有持续业务扩展需求的生产环境。

（3）大容量 Max 版：该架构在 Pro 版的基础上提供链的核心模块主备切换能力，并可通过多机部署交易执行器和接入分布式存储 TiKV，实现计算与存储的平行拓展。该架构中的一个节点由一系列微服务组成，但它依赖较高的运维能力，适合需要海量计算和存储的场景。

2. 多机拓展

在传统设计中，交易执行只可单机进行。FISCO BCOS v3.0 稳定版采用独创的确定性多合约并行方案（Deterministic Multi-Contract，DMC），能够在系统运行时自动进行交易冲突处理，并将多个交易调度到不同机器中并行执行，用户可通过拓展计算实例实现交易处理性能的平行拓展。

3. 支撑海量存储

FISCO BCOS v3.0 稳定版集成了 TiKV 存储引擎，并且在其基础上进行了二次开发，支持分布式事务性提交，结合 DMC 多计算实例，充分发挥存储性能，支撑海量数据上链。同时，本版本引入了 KeyPage 机制，参考内存页的缓存机制，将键值对组织成页的方式存取，解决了以往采用键值对方式存储数据时存储数据零散的问题，提升了数据访问的局部性，更适合大批量数据存取。

4. 特性继承与升级

FISCO BCOS v3.0 稳定版也继承了 v2.0 版本的诸多重要特性并进行了升级，主要包括以下几点。

（1）PBFT 共识算法：立即一致的共识算法，实现交易秒级确认。

（2）Solidity：支持至 0.8.11 版本。

（3）CRUD：采用表结构存储数据，在本版本中封装了更易用的接口，对业务开发更友好。

（4）AMOP：链上信使协议，借助区块链的 P2P 网络实现信息传输，实现接入区块链的应用间数据通信。

（5）落盘加密：区块链节点的私钥和数据加密存储于物理硬盘中，即使物理硬件丢失也无法解密。

（6）密码算法：内置群环签名等密码算法，可支持各种安全多方计算场景。

（7）区块链监控：实现区块链状态的实时监控与数据上报。

5. 全平台国密接入

FISCO BCOS v3.0 稳定版构建了通用国密基础组件，将国密算法、国密通信协议、国产密码机接入协议与 FISCO BCOS 的区块链基础数据结构封装于其中，基于该基础组件可快速开发出不同平台、不同操作系统和不同编程语言的 SDK，大幅提升了研发效率。

3.1.3 应用领域


3min

1. 政务领域

FISCO BCOS 作为金融级国产安全的区块链底层平台，在政务领域的应用展现了其强大的技术实力和创新能力。不仅提升了政府服务的效率和质量，也为政府部门之间的数据共享、信息公开、流程优化提供了强有力的技术支撑，展现了区块链技术在推动政府数字化

转型中的重要作用。

首先，在数据共享与交换方面，FISCO BCOS 通过构建安全、可靠的数据交换平台，实现了政府部门之间的信息互联互通，例如，珠三角征信链利用区块链技术，实现了跨区域、跨部门的信用信息共享，提高了征信数据的准确性和可用性，为金融机构和相关企业提供了更加精准的信用评估服务。

其次，在提升政务服务透明度方面，FISCO BCOS 通过区块链的不可篡改特性，为政府公开信息提供了安全保障。政府部门发布的政策文件、公告通知等信息一旦上链，任何个人和机构都无法擅自修改，确保了信息的真实性和权威性。

再次，在优化政务服务流程方面，FISCO BCOS 的应用有效地简化了政府服务流程，提高了办事效率，例如，在不动产登记领域，通过区块链技术实现了不动产信息的实时更新和共享，减少了传统纸质材料的流转，缩短了业务办理时间，提升了民众的办事体验。

此外，在保障数据安全方面，FISCO BCOS 采用了国密算法，为政务数据提供了更高级别的安全保护。政府部门在处理敏感数据时，可以利用区块链技术的加密和访问控制机制，有效防止数据泄露和滥用。

最后，在推动跨区域政务合作方面，FISCO BCOS 通过构建跨境数据互认系统，促进了不同地区之间的政务合作，例如，粤澳健康码跨境互认系统通过区块链技术，实现了粤港澳大湾区内的健康信息互认，为疫情防控和人员流动提供了有力支持。

2. 金融领域

FISCO BCOS 在金融领域的应用体现了区块链技术在提升金融服务效率、增强交易安全性、促进市场透明度及优化风险管理方面的显著优势。金融行业作为数据密集型行业，对数据的真实性、完整性和安全性有着极高的要求，而 FISCO BCOS 平台以其国产安全可控的特性，为金融行业提供了一个高度可靠的区块链解决方案。

在机构间对账方面，FISCO BCOS 通过构建一个去中心化的账本，实现了不同金融机构间交易信息的实时共享和同步，极大地提高了对账效率，降低了传统对账过程中的时间成本和人力成本。此外，区块链的不可篡改性也确保了对账数据的真实性和可靠性，降低了金融风险。

在供应链金融领域，FISCO BCOS 的应用促进了供应链上下游企业之间的信任建立，通过区块链技术记录和验证供应链中的交易行为和资金流向，为中小企业提供了更加便捷的融资渠道。同时，金融机构可以更准确地评估企业的信用状况，从而降低贷款风险。

在旅游金融领域，FISCO BCOS 的应用为旅游相关的金融服务提供了新的解决方案，例如，通过区块链技术记录旅游合同、保险单等信息，提高了旅游金融服务的透明度和安全性。同时，也为旅游者提供了更加便捷的支付和结算服务。

此外，FISCO BCOS 在跨境支付、资产数字化、征信等金融领域也有广泛应用，其高性能的交易处理能力、灵活的共识机制、全面的安全防护措施及丰富的开发工具和中间件，为金融行业提供了一个高效、安全、易用的区块链平台。

3. 医疗与教育领域

FISCO BCOS 在医疗和教育领域的应用，展现了区块链技术在提高数据管理效率、增强信息安全性、促进资源共享和优化服务流程方面的巨大潜力。在医疗领域，FISCO BCOS 的应用主要体现在健康数据管理、电子病历共享、药品供应链追踪和医疗审计等方面。通过

区块链技术，医疗机构能够安全地存储和共享患者的医疗记录，确保数据的真实性和完整性，同时保护患者隐私，例如，国家健康医疗大数据科创平台利用 FISCO BCOS 实现了医疗数据的安全存储和高效利用，为医疗研究和临床决策提供了有力支持。

在药品供应链管理中，FISCO BCOS 能够确保药品从生产到流通的每个环节都可追溯、可验证，从而有效防止假药流通，保障公众用药安全。此外，医疗审计方面，区块链的不可篡改性为医疗行为提供了可靠的审计轨迹，有助于提高医疗服务的透明度和公信力。

在教育领域，FISCO BCOS 的应用则体现在学籍管理、学历认证、在线教育和教育资源共享等方面。区块链技术的应用使学生的学籍和学历信息在教育机构之间安全、便捷地共享成为可能，同时，也为国际学历认证提供了一个高效、可靠的解决方案。在线教育平台可以利用 FISCO BCOS 确保课程内容和学习成果的真实性，提高远程教育的可信度。

教育资源共享方面，FISCO BCOS 可以构建一个去中心化的教育资源共享平台，促进优质教育资源的广泛传播和有效利用，缩小不同地区、不同群体之间的教育差距。通过区块链技术，教师和学生可以轻松地访问和贡献教育资源，实现知识的共创和共享。

4. 社会治理领域

通过区块链的透明性、不可篡改性和去中心化特性，FISCO BCOS 为社会治理现代化提供了强有力的技术支持。在不动产登记领域，FISCO BCOS 的应用简化了登记流程，确保了房产交易的安全性和效率，通过链上记录保障了交易信息的真实性和可追溯性。在社区治理中，它促进了居民参与和社区资源的高效管理，利用智能合约自动执行社区规定，提升了治理的公正性和透明度。此外，FISCO BCOS 在司法存证、文化版权保护等方面也发挥着重要作用，通过区块链技术确保了证据和版权信息的完整性与可靠性，加大了法律执行力度，维护了创作者的合法权益。这些应用不仅提高了社会治理的智能化和精准化水平，还有助于构建一个更加和谐、有序的社会环境，推动了社会治理体系和治理能力现代化。

3.2 FISCO BCOS 设计原理

3.2.1 系统架构概览


1min

FISCO BCOS v3.0 采用微服务模块化设计架构，总体上系统包含接入层、调度层、计算层、存储层和管理层 5 个方面，其设计架构如图 3-1 所示。

(1) 接入层：接入层主要负责提供区块链连接的能力，包括提供 P2P 能力的“对外网关服务”和提供给 SDK 访问的“对内网关服务”。在联盟链的体系中，“对外网关服务”管理了机构对外连接的出入口，负责机构级别的安全认证。“对内网关服务”则提供给机构内的客户端(应用端)访问入口。两个网关服务都可以平行扩展、多活部署、负载均衡，满足高可用要求。

(2) 调度层：调度层是区块链内核运转调度的“大脑中枢”系统，负责整个区块链系统运行调度，包括网络分发调度、交易池管理、共识机制、计算调度等模块，其中，网络分发模块主要与接入层实现互联通信功能，处理消息分发逻辑；交易池管理主要负责交易的接收、签名验证、淘汰等功能；共识机制负责交易排序、区块打包及对区块结果以分布式达成共识，确保一致性；计算调度则用于完成交易验证(核心是智能合约的验证)的调度处理，实现并行验证，是整个系统吞吐量的关键。

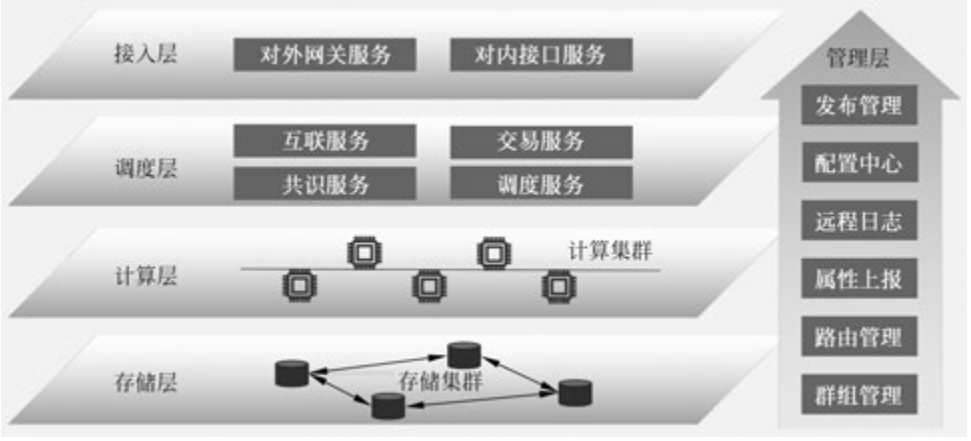

图 3-1　FISCO BCOS v3.0 设计架构

（3）计算层：这里主要负责交易验证，需要将交易解码放入合约虚拟机中执行，得到交易执行结果。交易验证是整个区块链的核心，尤其是基于智能合约的区块链系统，交易验证的计算可能需要花费较大的 CPU 开销，因此如何实现并行化交易验证，通过集群化模式实现交易验证计算的平行扩展是非常重要的。

（4）存储层：存储层负责落盘存储交易、区块、账本状态等数据，存储层重点关注如何支撑海量数据的存储，采用分布式存储集群的方式可实现存储容量可扩展。分布式存储业界已有许多稳定可复用的开源组件（如 TiKV）。

（5）管理层：管理层是为整个区块链系统各模块实现可视化管理的平台，包括部署、配置、日志、网络路由等管理功能。FISCO BCOS v3.0 系统架构基于开源微服务框架 Tars 构建，这层复用成熟的 Tars-Framework 来管理组件。


2min

3.2.2　区块链组件

1. 图形化的区块链管理工具

图形化的区块链管理工具（WeBank Blockchain Application Software Extension，WeBASE）是一套管理 FISCO BCOS 联盟链的工具集。WeBASE 提供了图形化的管理界面，屏蔽了区块链底层的复杂度，降低了区块链使用的门槛，大幅提高了区块链应用的开发效率，包含节点前置、节点管理、交易链路、数据导出、Web 管理平台等子系统。

2. 数据治理通用组件

数据治理通用组件（WeBankBlockchain-Data）是一套稳定、高效、安全的区块链数据治理组件解决方案，可无缝适配 FISCO BCOS 区块链底层平台。它由数据导出组件（Data-Export）、数据仓库组件（Data-Stash）、数据对账组件（Data-Reconcile）这 3 个相互独立、可插拔、可灵活组装的组件所组成，开箱即用，灵活便捷，易于进行二次开发。

3. 区块链多方协作治理组件

区块链多方协作治理组件（WeBankBlockchain-Governance）是一套轻量解耦、简捷易用、通用场景和一站式的区块链治理组件解决方案。首批开源的组件有账户治理组件（Governance-Account）、权限治理组件（Governance-Auth）、私钥管理组件（Governance-Key）和证书管理组件（Governance-Cert）。上述组件都提供了可部署的智能合约代码、易于

使用的 SDK 和可参考的落地实践 Demo 等交付物。

4. 区块链应用开发组件

应用开发组件(WeBankBlockchain-SmartDev)包含了一套开放、轻量的开发组件集,覆盖智能合约的开发、调试、应用开发等环节,包括智能合约库(SmartDev-Contract)、智能合约编译插件(SmartDev-SCGP)和应用开发脚手架(SmartDev-Scaffold)。开发者可根据自己的情况自由选择相应的开发工具,提升开发效率。

3.2.3 交易流程

交易是区块链系统的核心,负责记录区块链上发生的一切。区块链引入智能合约后,交易便超脱价值转移的原始定义,其更加精准的定义应该是区块链中一次事务的数字记录。无论大小事务都需要交易的参与。FISCO BCOS 的交易完整生命周期如图 3-2 所示。

1. 交易生成

用户的请求到达客户端后,客户端会构建出一笔有效交易,其交易生成流程如图 3-3 所示。交易中包括以下关键信息。

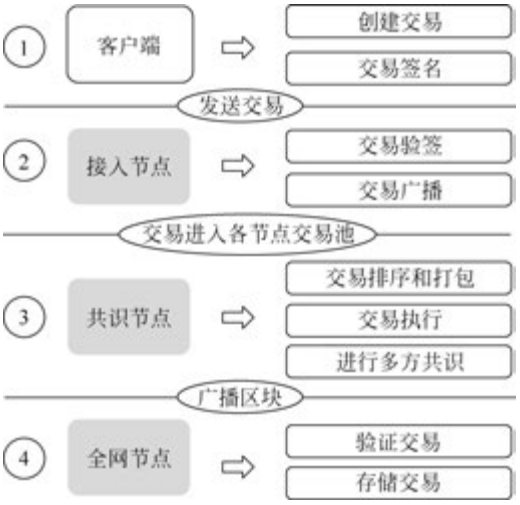

图 3-2 FISCO BCOS 的交易完整生命周期

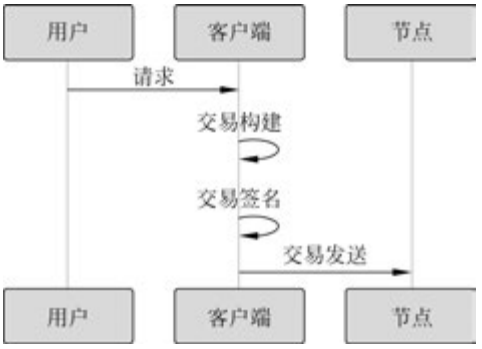

图 3-3 FISCO BCOS 交易生成流程

(1) 接收地址:FISCO BCOS 中的交易分为两类,一类是部署合约的交易,另一类是调用合约的交易。前者,由于交易并没有特定的接收对象,因此规定这类交易的接收地址固定为空;后者,则需要将交易的接收地址置为链上合约的地址。

(2) 交易相关的数据:一笔交易往往需要用户提供一些输入信息来执行用户期望的操作,这些输入信息会以二进制的形式被编码到交易中。

(3) 交易签名:为了表明交易确实是由用户发送的,用户会向 SDK 提供私钥来让客户端对交易进行签名,其中私钥和用户账户是一一对应的关系。

2. 交易池

区块链交易被发送到节点后,节点会通过验证交易签名的方式来验证这一笔交易是否合法。若这一笔交易合法,则节点会进一步检查该交易是否重复出现过,若从未出现过,则将交易加入交易池缓存起来。若交易不合法或交易重复出现,则将直接丢弃交易。交易池

的流程如图 3-4 所示。

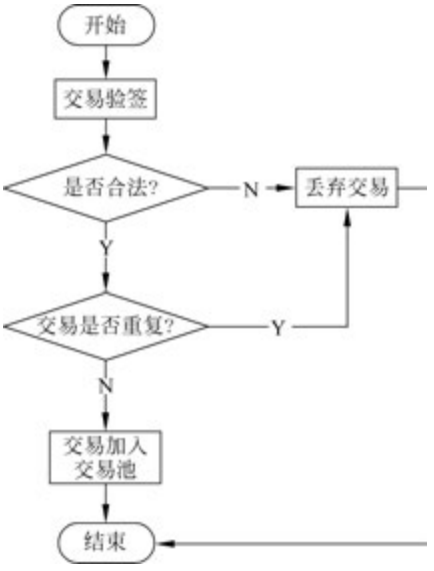

图 3-4　交易池的流程

3. 交易广播

节点在收到交易后，除了会将交易缓存在交易池外，节点还会将交易广播至该节点已知的其他节点。为了能让交易尽可能地到达所有节点，其他收到广播的节点，也会根据一些精巧的策略选择一些节点，对交易再一次进行广播，例如对于从其他节点转发过来的交易，节点只会随机选择 25%的节点再次广播，因为这种情况一般意味着交易已经开始在网络中被节点接力传递，缩减广播的规模有助于避免因网络中冗余的交易太多而出现的广播风暴问题。

4. 交易打包

为了提高交易处理效率，同时也为了确定交易之后的执行顺序保证事务性，当交易池中有交易时，Sealer 线程负责从交易池中按照先进先出的顺序取出一定数量的交易，组装成待共识区块，随后待共识区块会被发往各个节点进行处理。交易打包的流程如图 3-5 所示。

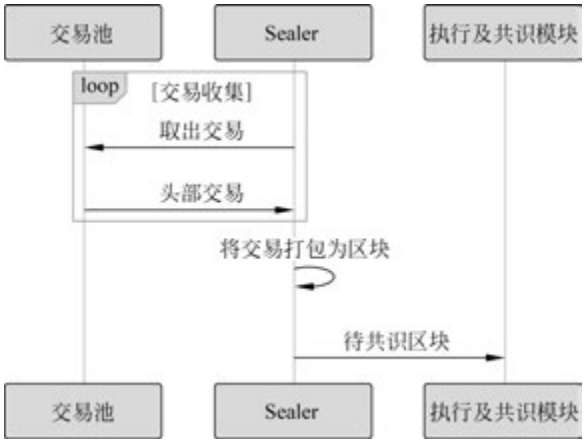

图 3-5　交易打包的流程

5. 交易执行

节点在收到区块后会调用区块验证器把交易从区块中逐一取出来执行。如果是预编译合约代码，则验证器中的执行引擎会直接调用相应的 C++功能，否则执行引擎就会把交易交给 EVM(以太坊虚拟机)或 WASM 执行。交易可能会执行成功，也可能因为逻辑错误或 Gas 不足等原因执行失败。交易执行的结果和状态会封装在交易回执中返回。交易执行的流程如图 3-6 所示。

6. 交易共识

区块链要求节点间就区块的执行结果达成一致才能出块。在 FISCO BCOS 中一般采用 PBFT 算法保证整个系统的一致性，其大概流程是：各个节点先独立执行相同的区块，随

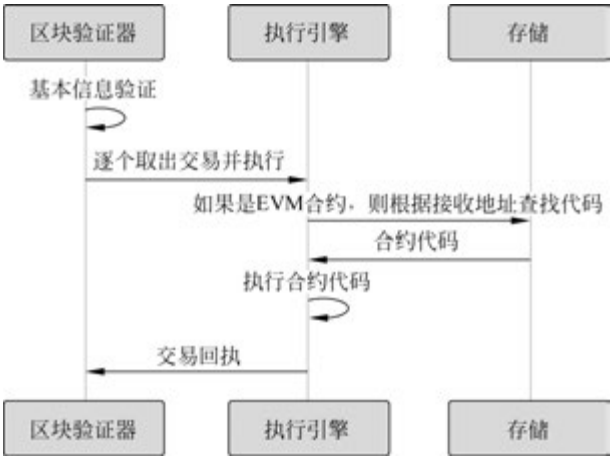

图 3-6 交易执行的流程

后节点间交换各自的执行结果，如果发现超过 2/3 的节点得出了相同的执行结果，则说明这个区块在大多数节点上取得了一致，节点便会开始出块。

7. 交易落盘

在共识出块后，节点需要将区块中的交易及执行结果写入硬盘永久保存，并更新区块高度与区块哈希的映射表等内容，然后节点会从交易池中剔除已落盘的交易，以开始新一轮的出块流程。用户可以通过交易哈希等信息，在链上的历史数据中查询自己感兴趣的交易数据及回执信息。

8. 交易原子性

一笔交易在多个区块链节点上对数据状态的更新是原子性的。当出现外界影响（如断电、重启、网络波动等异常场景）时会造成达成共识失败，各区块链节点会丢弃当前的执行结果，并不会将该交易对状态的修改落盘。交易在每个节点上对数据状态更新的落盘行为必须在节点达成共识之后进行，进而保证了交易的原子性。

3.2.4 同步模块

同步是区块链节点非常重要的功能。它是达成共识的辅助，给达成共识提供必需的运行条件。同步分为交易的同步和状态的同步。交易的同步，确保了每笔交易能正确地到达每个节点。状态的同步，能确保区块落后的节点能正确地回到最新的状态。只有持有最新区块状态的节点，才能参与到达成共识中去。

1. 交易广播

交易同步是让区块链上的交易尽可能地到达所有的节点。为在达成的共识中将交易打包成区块提供基础。一笔交易（tx1），从客户端上发往某个节点，节点在接收到交易后会将交易放入自身的交易池（TxPool）中供达成的共识去打包。与此同时，节点会将交易广播给其他的节点，其他节点收到交易后，也会将交易放到自身的交易池中。

通常会在极小的概率下出现某交易无法到达某节点的情况，此情况是允许的。让交易尽可能地到达更多的节点，是为了让此交易尽快地被打包、达成共识、确认，尽量地让交易能够更快地得到执行的结果。当交易未到达某个节点时，只会使交易的执行时间变长，不会影

响交易的正确性。在达成共识流程中会验证 leader 打包的区块交易列表，如果本地出现了交易缺少的情况，则会主动向 leader 请求缺少的交易。

2. 状态同步

状态同步是让区块链节点的状态保持在最新。区块链的状态的新旧，是指区块链节点当前持有数据的新旧，即节点持有的当前区块块高的高低。若一个节点的块高是区块链的最高块高，则此节点就拥有区块链的最新状态。只有拥有最新状态的节点，才能参与到达成共识中去，尝试在下一个新区块达成共识。

在一个全新的节点加入区块链或一个已经断网的节点恢复了网络时，此节点的区块落后于其他节点，状态不是最新的。此时就需要进行状态同步。需要状态同步的节点（Node 1）会主动向其他节点请求下载区块。整个下载过程会将下载的负载分散到多个节点上。状态同步的整个流程如图 3-7 所示。

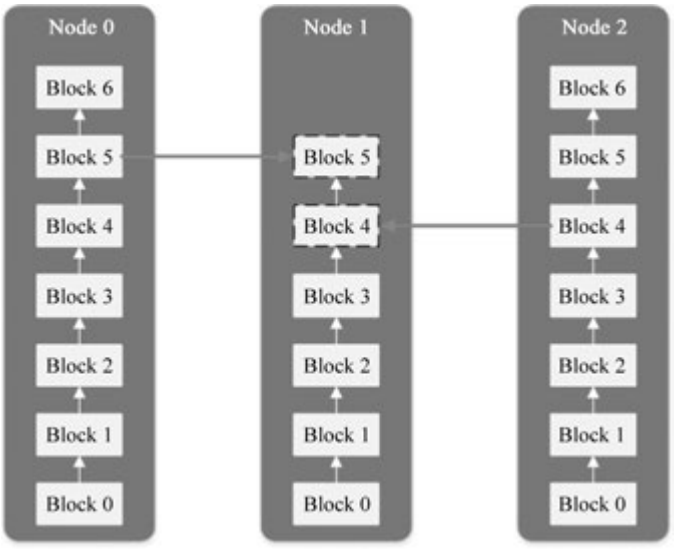

图 3-7　状态同步流程

3. 下载队列

区块链节点在运行时会定时地向其他节点广播自身的最高块高。节点收到其他节点广播过来的块高后会和自身的块高进行比较，若自身的块高落后于此块高，就会启动区块下载流程。

区块的下载通过请求的方式完成。进入下载流程的节点会随机地挑选满足要求的节点，发送需要下载的区块区间。收到下载请求的节点会根据请求的内容，回复相应的区块。

当收到回复区块的节点后，在本地维护一个下载队列，用来对下载下来的区块进行缓冲和排序。下载队列是一个以块高为顺序的优先队列。下载下来的区块会被不断地插入下载队列中，如果队列中的区块能连接上节点当前本地的区块链，则将区块从下载队列中取出，真正地连接到当前本地的区块链上。整个下载队列的流程如图 3-8 所示。


1min

3.2.5　存储设计

存储层需要能够满足 Air、Pro 和 Max 这 3 个版本的不同设计目标，为此 FISCO BCOS

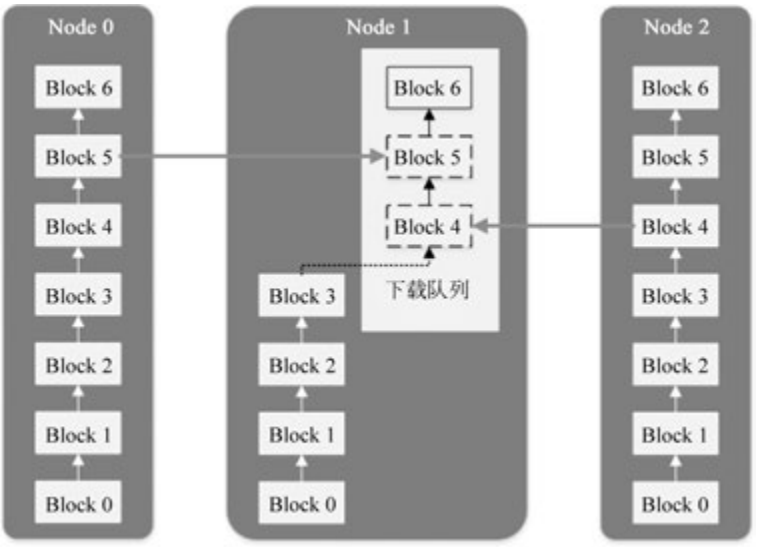

图 3-8 下载队列的流程

使用同一套接口来屏蔽不同版本存储的具体实现。对于 Air 和 Pro 版本，存储层使用 RocksDB 来满足其轻便和高性能的需求，对于 Max 版本通过接入能够支持水平扩展的分布式数据库支撑大规模数据存储的需求则选择了 TiKV，通过 Raft 协议保证了多副本数据的一致性及高可用性。整体存储服务设计如图 3-9 所示。

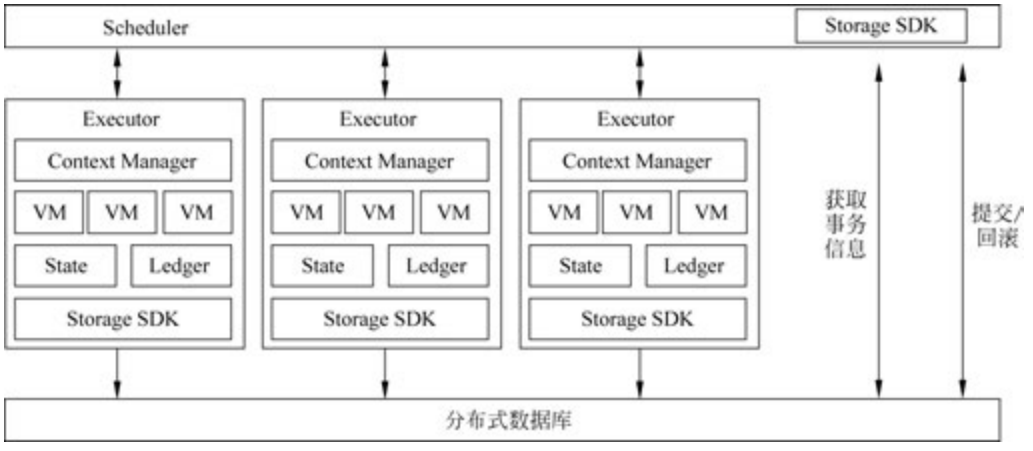

图 3-9 存储服务设计

Air、Pro 和 Max 版本的区别在于其使用的 Storage SDK 内部的具体实现是不同的，对于 Air 和 Pro 版本，在初始化时会创建基于 RocksDB 封装的实现，而对于 Max 版本则提供基于 TiKV 封装的实现，同时保留定制存储的能力，用户可以基于具体的业务需求接入其他数据库。

3.2.6 安全控制

为了保障节点间的通信安全性，以及对节点数据访问的安全性，FISCO BCOS 引入了节点准入机制、CA 黑名单和权限控制 3 种机制，在网络和存储层面上做了严格的安全

控制。

在网络层面安全控制方面，节点使用 SSL 连接，保障了通信数据的机密性。引入网络准入机制，可将指定群组的作恶节点从共识节点列表或群组中删除，保障了系统安全性。通过群组白名单机制，保证每个群组仅可接收相应群组的消息，保证群组间通信数据的隔离性。引入 CA 黑名单机制，可及时与作恶节点断开网络连接。提出权限治理体系机制，灵活、细粒度地控制外部账户部署合约和创建、插入、删除、更新用户表的权限。

在存储层面安全控制方面，基于分布式存储，提出分布式存储权限控制的机制，以灵活、细粒度的方式有效地进行权限控制，设计并实现了权限控制机制限制外部账户（tx. origin）对存储的访问，权限控制范围包括合约部署、表的创建、表的写操作。