中国区块链技术和产业发展论坛标准

CBD-Forum-002-2019

区块链 跨链实施指南

Blockchain—Cross-Blockchain implementation guidelines

2019-07-19 发布　　2019-07-19 实施

中国区块链技术和产业发展论坛　　发 布

目　　次

前　言

本标准按照 GB/T　1.1-2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国区块链技术和产业发展论坛提出。

本标准负责起草单位：上海复星高科技（集团）有限公司、中国电子技术标准化研究院、上海万向区块链股份公司、深圳前海微众银行股份有限公司、厦门安妮股份有限公司、中国平安保险（集团）股份有限公司、上海金丘实业股份有限公司、福建省海峡区块链研究院、易见供应链管理股份有限公司、深圳华大基因科技有限公司、北京京东尚科信息技术有限公司。

本标准主要起草人：鞠鹏、李鸣、廖娅伶、赵阳、李斌、陈家乐、徐磊、莫楠、李昊轩、孙琳、李佳秾、刘天成、朱振博、郝玉琨、黄浩、高林挥、黄艳挺、郝汉　杨胜、陶祥忍、张作义、杨梦、潘光明、张龙、刘恩科。

使用帮助信息：任何单位和个人在使用本标准的过程中，若存在疑问，或有对本标准的改进建议和意见，请与中国电子技术标准化研究院（中国区块链技术和产业发展论坛　秘书处）联系。

电话：010-64102801/2804；电子邮件：cbdforum@cesi.cn

通信地址：北京东城区安定门东大街 1 号（100007）

为了推动本标准的持续改进，使其内容更加贴近用户组织的实际需求，欢迎社会各方力量参加本标准的持续改进，本标准的更多信息欢迎关注中国区块链技术和产业发展论坛官方网站和公众号。

http://www.cbdforum.cn

区块链 跨链实施指南

1 范围

本标准规定了区块链的跨链实施指南，给出了跨链实施的应用构建、应用运行、应用评估和实施改进过程。

本标准为计划应用跨链的组织提供参考，为计划实施跨链的组织提供指导。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注明日期的引用文件，仅注明日期的版本适用于本文件。凡是不注明日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25000.10-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型

CBD-Forum-001-2017 区块链 参考架构

3 术语和定义

CBD-Forum-001-2017界定的以及下列术语和定义适用于本文件。为了方便使用，以下重复列出了CBD-Forum-001-2017中一些术语和定义。

3.1

共识算法 consensus algorithm

区块链系统中各节点间为达成一致采用的计算方法。

[CBD-Forum-001-2017，定义2.2.3]

3.2

分布式账本 distributed ledger

可以在多个站点、不同地理位置或者多个机构组成的网络里实现共同治理及分享的资产数据库。

3.3

智能合约 smart contract

以数字形式定义的能够自动执行条款的合约。

注：在区块链技术领域，智能合约是指基于预定事件触发、不可篡改、自动执行的计算机程序。

[CBD-Forum-001-2017，定义2.2.7]

3.4

跨链技术 cross-blockchain technology

实现多个区块链或分布式账本之间信息交换的技术。

3.5

锚定节点 anchor peer

在跨链实现时选定的信息交换的节点。

4 缩略语

下列缩略语适用于本文件。

NS：公证人机制（Notary Schemes）

HL：哈希锁定（Hash-locking）

SC：侧链（Sidechains）

DPKC：分布式私钥控制（Distributed Private Key Control）

5 跨链实施框架

跨链实施框架包含跨链应用构建、跨链应用运行、跨链应用评估，和跨链实施改进，具体包括：

a) 跨链应用构建包括跨链应用设计和跨链应用研发；

b) 跨链应用运行包括部署、触发、执行、维护、废止；

c) 跨链应用评估包括安全审计和质量评价；

d) 跨链实施改进包括对应用构建和运行的改进。

跨链实施框架见图 1。

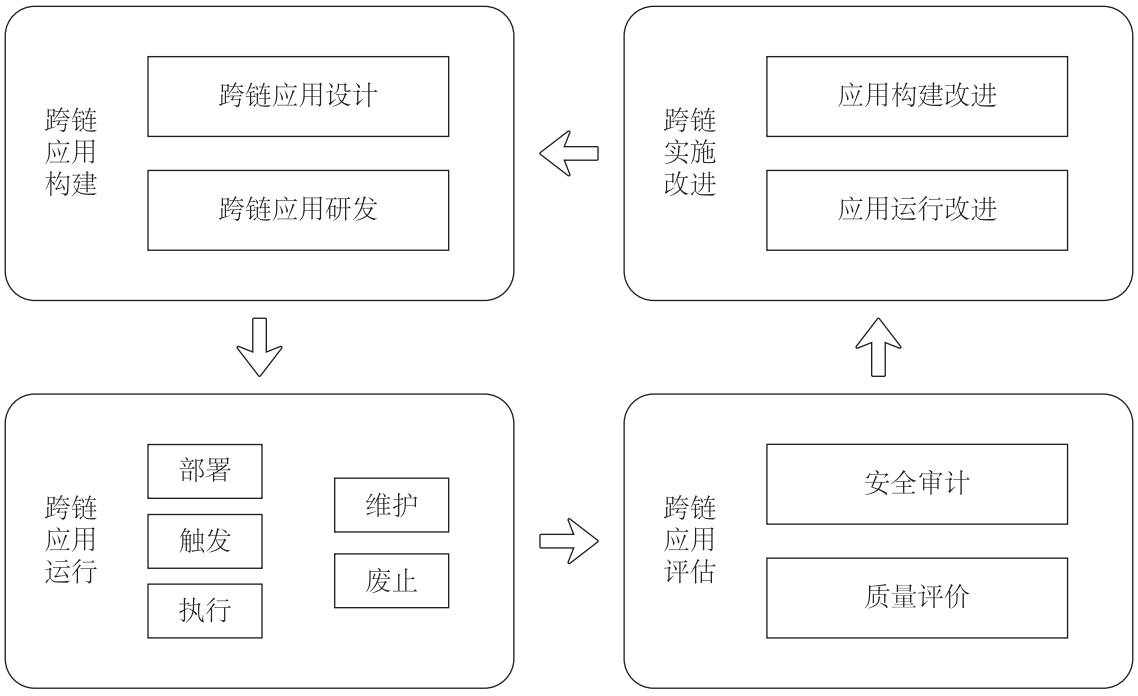

图 1 跨链实施框架

6 跨链实施过程

6.1 应用构建

6.1.1 跨链应用设计

6.1.1.1 跨链设计原则

跨链设计应遵循以下原则：

a) 松耦合

跨链通道或锚定节点受损时，应不影响区块链的正常运行；

b) 可扩展

跨链架构可支持多个同构或异构区块链网络的链接；

c) 互操作

跨链应用可提供区块链服务用户跨链创建账户、事务、合约等活动的跟踪、审计及其他监管功能；

d) 安全可靠

跨链应用运行时，应满足信息的完整性、数据的隐私性和应用的可靠性。

6.1.1.2 锚定节点选择原则

锚定节点选择应遵循以下原则：

a) 节点的可信任程度

锚定节点的选择应确保被选择节点在区块链系统中的合法性地位及交易数据完整性。当多个节点的合法性地位及交易数据完整性存在不一致时，应优先考虑选择合法性地位高和交易数据最为完整的节点担任锚定节点。

在许可链系统和非许可链系统中，应充分考虑各节点的合法性地位及交易数据完整性的实现程度存在的差异。

b) 节点的可用性

锚定节点的选择应确保跨链业务的高可用性，优先选择高可用度的区块链节点，同时考虑：

1) 待选节点的可用性监测；
2) 已选中节点的可用性监测；
3) 锚定节点的动态切换；
4) 锚定节点的动态增减；
5) 复杂跨链系统中的跨链环路检测及过滤。

c) 节点的服务性能

锚定节点的选择应确保跨链业务的整体性能最优。当有多个节点可供选择时，宜优先选择当前业务规则下性能最优的区块链节点担任锚定节点。

当跨链性能要求较高时，可考虑将多个锚定节点进行绑定，共同对上层提供跨链业务服务。多个锚定节点间可采取负荷分担、主备轮循等业务调度分发机制。

当存在复杂多链互联互通业务场景时，锚定节点应提供跨网业务转发功能。锚定节点的选择宜考虑通过专门的锚定节点转发协议来实现。

6.1.2 跨链应用研发

跨链应用研发是指构建跨链应用中功能组件的研发过程，跨链应用应：

a) 具备鉴权和授权能力，实现可审计、可追溯；

b) 具备安全可靠的通信协议，在传输过程中避免数据泄漏或遭到篡改；

c) 提供管理和维护接口。

6.2 跨链应用运行

6.2.1 概述

跨链应用运行包括部署、触发、执行、维护、废止五个步骤，见图 2。

图 2 跨链应用运行流程

6.2.2 部署

跨链应用部署是指部署锚定节点以及跨链相关应用的过程。

6.2.3 触发

跨链应用触发是指区块链服务使用方使用区块链服务时发起跨链应用的调用。根据区块链功能架构，跨链应用的触发可以分为三层：

a) 用户层触发

在用户层使用区块链服务的区块链服务客户发起跨链交互的过程；

b) 应用层触发

在应用层跨链业务逻辑被调用的过程，包括事件触发、时间触发和交易触发等；

c) 核心层触发

在核心层一个链产生的事件传递到另一个链并被其接收、处理的过程。

6.2.4 执行

跨链应用执行是指执行跨链应用业务逻辑的过程。在此过程中，根据跨链请求在各个链上分别执行业务逻辑，执行结果应具备事务一致性。

6.2.5 维护

跨链应用维护是指维护已部署跨链应用的过程。该过程由跨链应用服务提供方调用，在锚定节点及跨链应用涉及的多个链上全部启用后生效。

6.2.6 废止

跨链应用废止是指废弃已部署跨链应用的过程。该过程由跨链应用服务提供方调用，在锚定节点及

跨链应用涉及的多个链上全部启用后生效，跨链应用废止应满足以下要求：

a) 跨链应用废止时，对于该应用上正在跨链执行的事务应有统一的处理规则；

b) 跨链应用废止后，应在相关的区块链网络中保存被终止的跨链应用版本。

6.3 跨链应用评估

6.3.1 安全审计

安全审计包括业务及技术框架安全审计、源代码安全审计、部署审计、运维审计及相关的应急响应审计：

a) 业务及技术框架安全审计应包括但不限于业务及技术框架是否能确保事务的原子性、一致性、不可抵赖性及服务的安全性；

b) 源代码安全审计可通过人工阅读源代码和代码审计工具的方式，对跨链服务代码进行测试分析；

c) 部署及运维审计可通过相关部署及运维工具，如自动化构建工具、日志分析工具等对跨链服务进行分析；

d) 应急响应审计是指审计跨链应用服务提供方的应急响应机制和应急预案。在发生跨链功能漏洞或故障时，能否通过应急响应机制和应急预案避免影响扩大，并分析问题和修复故障。

6.3.2 质量评价

跨链应用的质量模型参考 GB/T 25000.10-2016《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 10 部分：系统与软件质量模型》中的质量模型，评价要素包括功能、性能、可靠性、安全性、可维护性、可移植性和互操作性。见图 3。

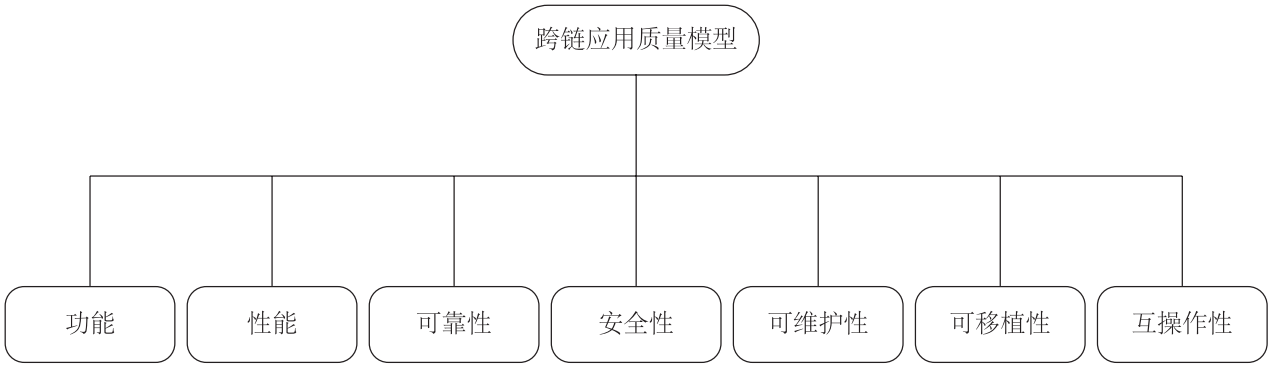

图 3 跨链应用质量模型

6.4 跨链实施改进

跨链应用的实施改进包含但不限于应用构建和应用运行的改进。改进的依据包含但不限于：

a) 适用的标准、政策、法律法规、目标和其他要求发生变化；

b) 跨链应用评估的结果与实际要求不匹配；

c) 跨链应用实施和评价提出的改进要求；

d) 与跨链有关的科研成果、新技术等方面的信息；

e) 顾客及其他相关方反馈的建议；

f） 测试、检验、试验报告；

g） 跨链实施时的纠正措施和预防措施。

附 录 A
（资料性附录）
主流跨链技术

A.1 跨链技术演进

随着区块链技术的演进与发展，2012 年出现了跨账本互操作协议（Interledger Protocol，ILP），通过第三方公证人的方式实现了跨账本交互，该方案是公证人机制（notary schemes）的代表。

2014 年，比特币核心开发团队提出锚定式侧链（Pegged Sidechains）跨链交互方案，引入一条与主链双向锚定（Two-way peg）的侧链，实现跨链资产转移。

2015 年出现的哈希时间锁（Hashed Timelock）机制，实现了比特币链下快速交易通道。2017 年 Interledger(ILP) 引入了哈希时间锁协议（HTLAs，Hashed-Timelock Agreements）来支持闪电网络的互操作性。

2016 年 BTC Relay 方案发表，基于侧链跨链（Sidechains）方案实现了比特币到以太坊的单向跨链连通。

同样在 2016 年 Vitalik Buterin 发表的《Chain Interoperability》对区块链互操作问题做了全面和深度的分析。将跨链策略归纳为以下三种：

a) 中心化或多重签名的公证人机制 (Centralized or multisig notary schemes)

b) 侧链 / 中继模式 (Sidechain/relays)

c) 哈希锁模式 (Hash-locking)

进入 2017 年，跨链方案出现了一些不同的方向：

分布式私钥控制技术，主要着眼于建立一条非许可链并将其连接到不同的区块链上，通过密钥控制技术来将其他链上的资产映射或移入 / 移出至该非许可链上。

BCOS 系列平台则利用同构多链结构实现跨链并提升性能。

A.2 跨链技术

总体来说，跨链技术仍未成熟，有巨大的发展和创新空间，是未来区块链发展的重点。

a) 公证人机制（Notary Schemes）

公证人机制（Notary Schemes）通过借助第三方“公证人”，在两个不同区块链系统之间实现数字资产转移。其中，“公证人”由一个或多个可信实体组成，这些实体可能是两个系统之间的连接器，也可能是交易双方均信任的第三方节点，能够为跨链的交易双方提供交易正确性、唯一性的验证服务。在处理资产转移的过程中，“公证人”可以是根据事件来主动接收并自动执行，也可以是被动发布执行签署消息；通常情况下，方案可以部署并使用相关（多重）签名算法和共识协议来保证资产转移过程中的可信度。

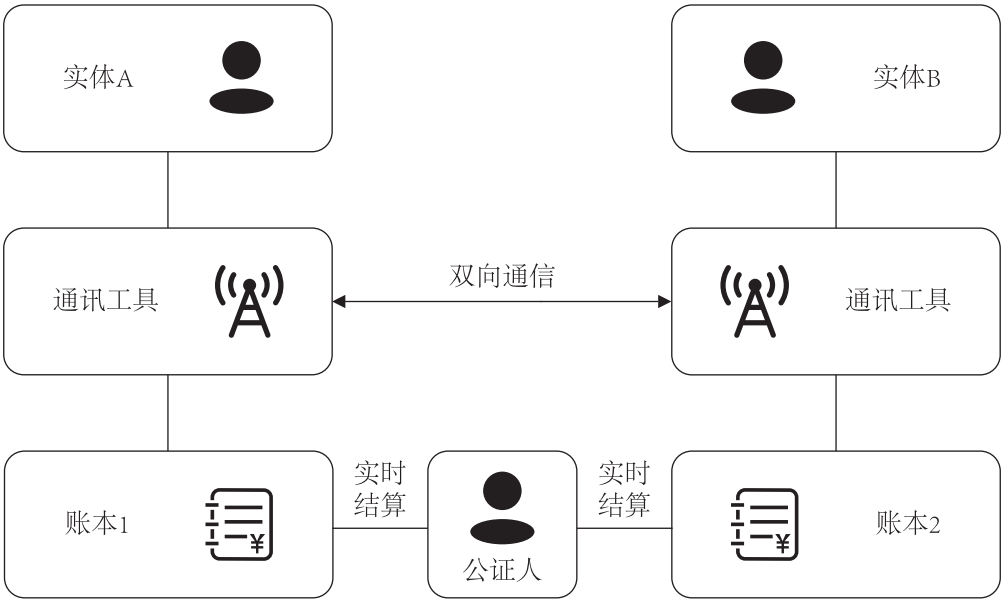

图 A1　公证人机制

b)　侧链 / 中继技术（Sidechains/Relays）

侧链 / 中继技术（Sidechains/Relays）是一种无需可信第三方参与验证、接收链能够自行检验交易数据且具有可扩展性的跨链技术。在接收链中创建智能合约，该智能合约能够以发起链的区块头为输入，使用发起链内的标准验证方式来检验区块头是否满足共识算法规范要求。一旦核实该区块头已最终确定，就可以通过区块头对应的默克尔树分支来验证相关交易或账户。侧链 / 中继技术能够用来进行资产转移、原子互换和其他复杂用例。

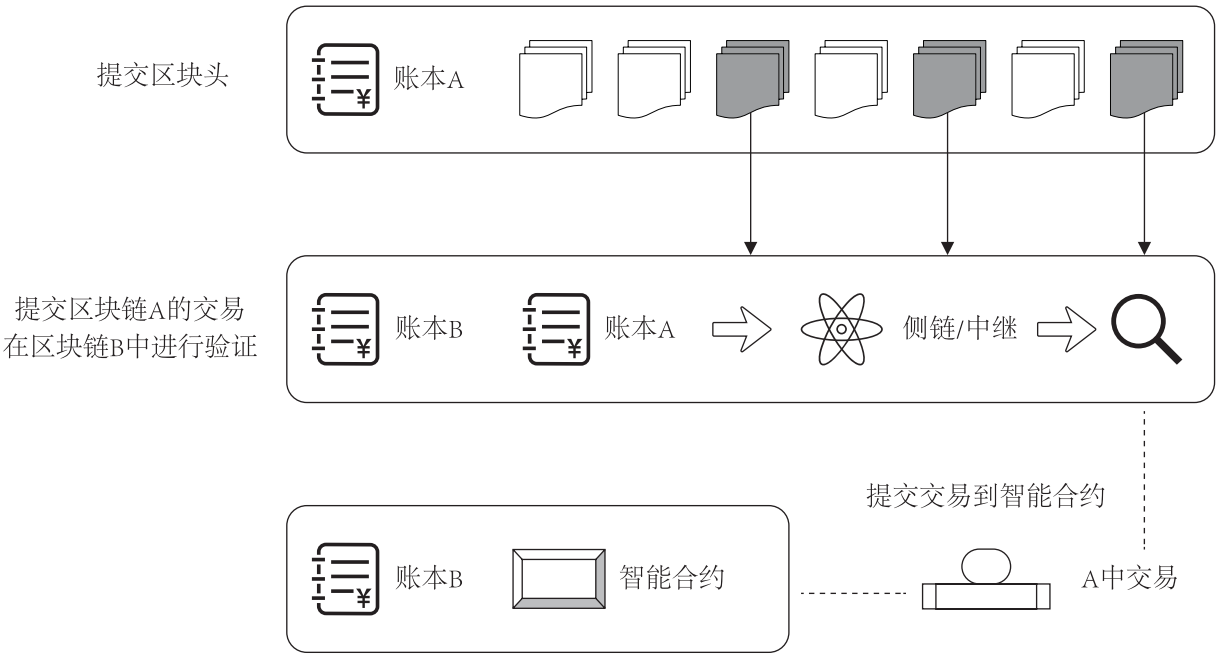

图 A2　侧链 / 中继技术

c） 哈希锁定（Hash-locking）

哈希锁定（Hash-locking）是一种能够构建可扩展微支付通道的跨链技术方案，能够在无需可信公证人情况下实现数字资产交换。在方案中，发起者首先随机选取秘密值，并计算秘密值的哈希值，然后将哈希值发送给响应者；发起者和响应者将各自数字资产锁定在智能合约中，如果一方在规定时间内无法提供秘密值，则合约中的锁定资产将被对方收回。此外，借助状态通道高效性，哈希锁定可以与之结合实现快速支付。需要注意的是，哈希锁定适用于资产交换的场景，但是不适用于不同链之间的资产转移和预言机用例：哈希锁定的原子互换协议保证同一条链中的资产总量保持不变，不能将一条链的资产转移到另一条链中；跨链预言机是一种只读的被动操作，而哈希锁定是一种双方主动操作，两者有着本质的区别。

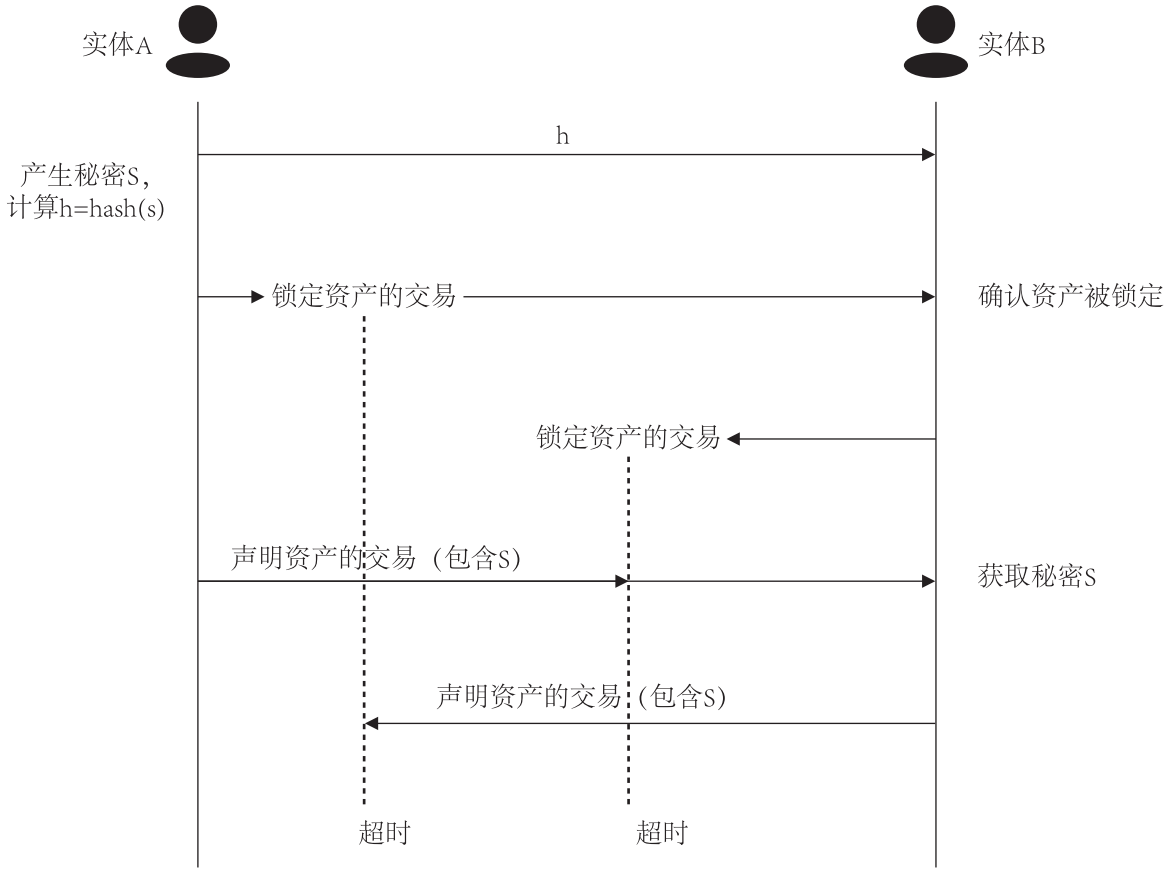

图 A3　哈希锁定

d） BCOS/FISCO　BCOS 同构链跨链技术

BCOS/FISCO　BCOS 两大平台（以下简称 BCOS 系列平台）由国内多家著名企业联合开发，所有代码现已完全开源并持续迭代中。BCOS 系列平台支持多链架构设计，在开源社区中也提供了基础分组策略和实现、路由模块和并行多链的构建工具等。开发者可根据业务场景需求灵活设计不同的分组，如根据机构维度、用户维度、交易维度，甚至是时间维度等，从而链的数量在理论上可以无限扩大。

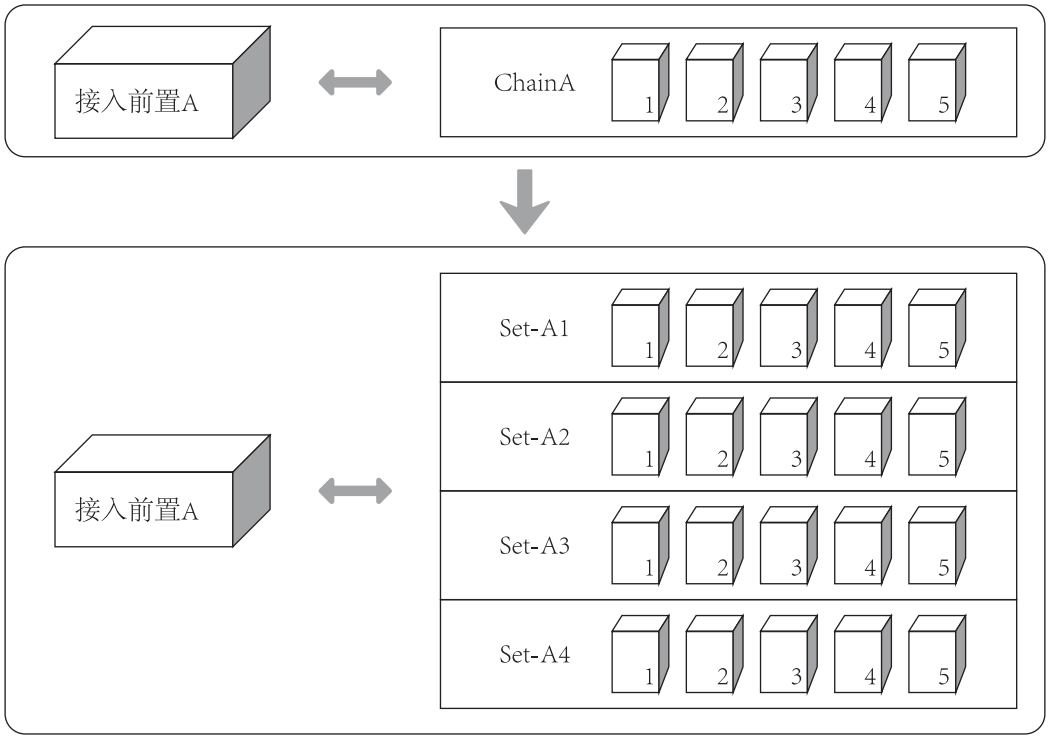

图 A4　BCOS 系列平台的并行计算多链架构

而采用多链架构之后，其节点操作、跨链交互可基于网络地址和通过路由规则实现，从而执行跨链读写。在跨链交互环节，需要重点关注分组间的通信可靠性、分布式事务完整性和一致性，以及分组之间可验证、不可篡改、可追溯的互信性和交易安全性。在具体设计中，建议同一个区块链网络里的多个分组在业务逻辑和配置尽可能地高度一致，在商业规则、运营管理上都使用统一策略，即尽可能确保是同构链。

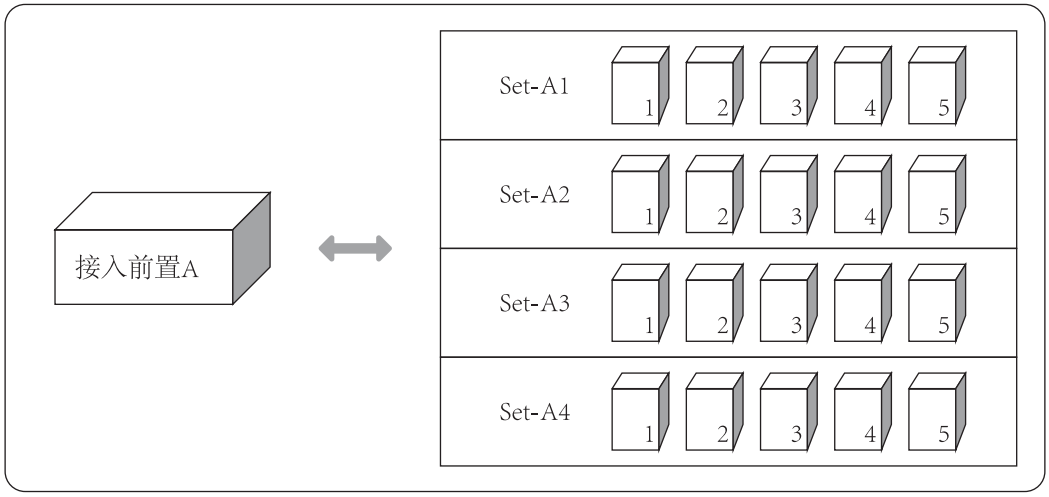

图 A5　BCOS 系列平台的跨链交互

以真实生产环境的高并发商业需求为例：当出现大量的独立用户帐户和少数集中的一个或多个热点帐户产生交易的情况时，如用户往某个热销中的商户付款，或者用户频繁从某个帐户中提现或者获取

优惠券、积分或者其他资产等，需要进行海量的用户交易、汇总对账和清结算流程等，这时就可以采用BCOS的多链架构和跨链交互解决方案，构建多条“用户交易链”、“热点账户链”、“路由链”等，进行多次跨链双向通信，且在不同的链上完整地执行共识确认。

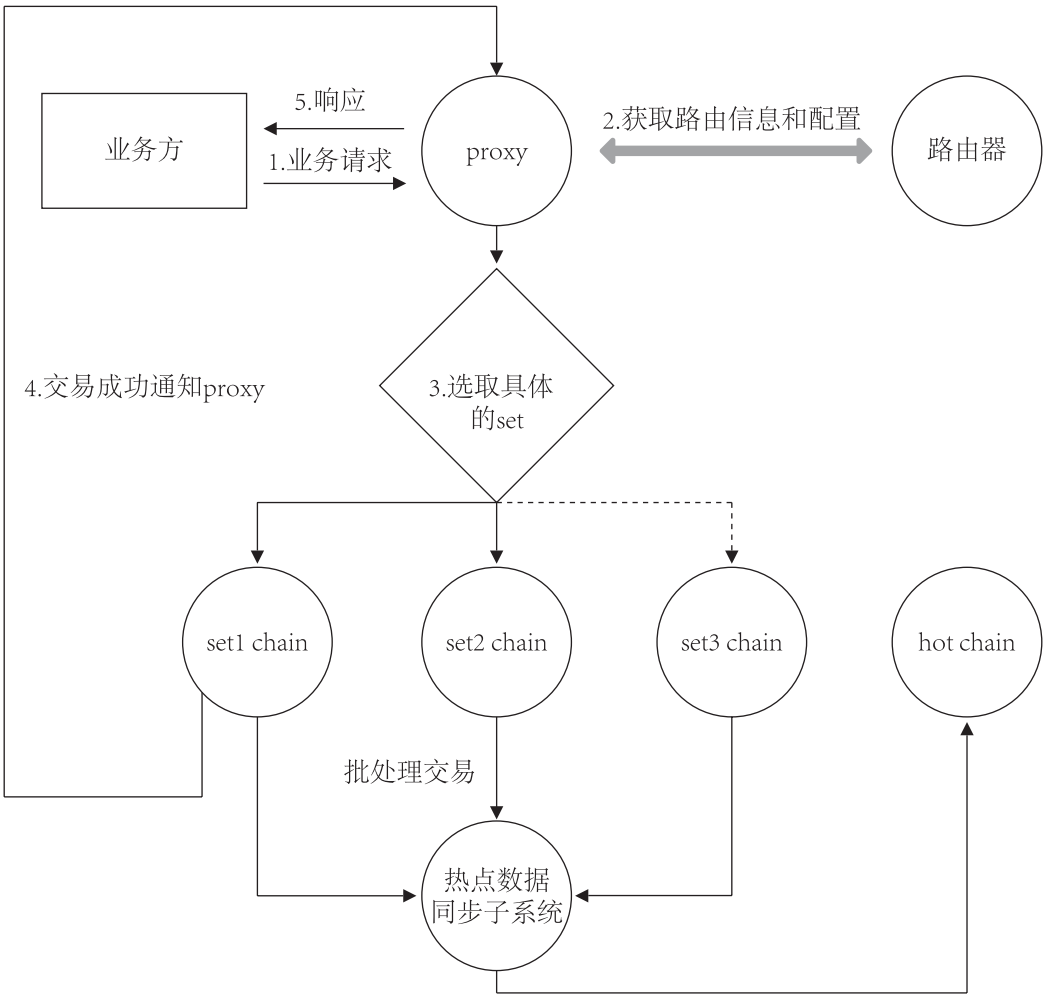

图 A6　高并发需求下的多链架构和跨链交互示意图

总之，通过同构链上的多链并行架构和跨链交互设计，BCOS系列平台在存储方面可实现分布式存储，能支持海量服务的存储需求，提高存储访问速率，节省存储消耗；在性能方面，实测单一条链就可以达到数千TPS，而在多链架构下的并行计算性能在理论上则无上限；在分布式程度方面，多链的分组模式可支持根据节点数量进行水平扩容，因此理论上节点数量也是不受限制的。目前，BCOS系列平台通过服务金链盟的百余家单位，已经支持了数百个区块链应用场景，在实践中印证了平台与架构的可行性与健壮性。其下一步的愿景是通过多链与跨链技术，有效促进多个联盟间进行协同合作、共同搭建公众联盟链生态、实现新型分布式商业模式。

参 考 文 献

[1] CBD-Forum-001-2017 区块链 参考架构

[2] GB/T 25000.10-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型

CBD-Forum-002-2019

电话：010-64102801/2804
电子邮件：cbdforum@cesi.cn
网址：http://www.cbdforum.cn