L0：一种树型分布式账本系统

V0.8

北京博晨技术有限公司

2017年6月16日

目录

第一章 引言

自比特币诞生以来，其背后的支撑技术区块链（Blockchain）吸引了越来越多的关注，被认为是构建下一代价值互联网的核心技术。区块链的发展同时带动了分布式账本技术（Distributed Ledger Technology，或DLT）的兴起。一般来说，大体可以认为这两个概念是互通的，指的是同一类技术。严格点理解，可以认为区块链是分布式账本技术的一种实现方式。

虽然分布式账本技术的发展非常迅速，但目前整体上还处于早期阶段，远不够成熟。有些核心的技术瓶颈没有突破，阻碍了该项技术的大规模应用，其中，以性能瓶颈尤为突出。在现有区块链技术中，区块链的处理能力主要受制于共识算法的性能，而共识算法性能又受制于系统节点的规模和单节点的处理能力。在目前的技术水平下，单条区块链性能优化提升的空间非常有限，且存在性能极限，这严重制约了分布式账本技术在大规模、高并发、低延迟的交易型业务场景中的应用。可以预见，随着数字经济的高速发展，未来交易的频率和规模会远远超出当前的水平，性能瓶颈是分布式账本技术需解决的首要问题之一。

LO是北京博晨技术有限公司（以下简称：博晨）推出的具有自主知识产权的分布式账本系统。我们开创性地设计了树型分层的分布式账本架构。LO是多链的有机组合，通过创新的跨链共识与分层交易机制，以及对账户和交易的全新分类，突破了传统单链结构的性能及存储瓶颈，理论上支持任意规模的网络和任意级别的并发，同时为现实场景中热点账户性能瓶颈的解决提供了内生的支持。

1.1. 定位

1.1.1. 自主

L0是博晨源代码级自主研发的分布式账本系统，拥有创新的理念和多项核心专利技术。在整体架构，共识算法，智能合约，账本存储等关键点均有创新的技术实现。

1.1.2. 开放

L0是一个开源、开放的系统，我们深知，用于构建多方信任的底层技术，如果不够开放，信任便无从谈起。我们将致力于推动开放、共赢的价值互联网生态系统的构建。

1.1.3. 高效

我们开创性地提出了以树型分层结构为核心架构的多链网络，能够实现分布式账本系统的大规模并发交易处理。

1.1.4. 一致性

一致性是确保分布式账本正常运作，并降低交易欺诈风险的核心特性。L0通过创新的跨链共识算法、跨层汇总交易等设计，保证了网络账本数据的一致性。

1.1.5. 扩展性

节点及账本规模的动态扩展是分布式账本系统大规模商用所必备的关键特性。L0系统在实际应用中，可根据需求动态调整账本规模，实现业务的弹性负载。

1.6. 安全性

基于密码学、PKI，以及共识算法的可靠性，保证节点准入，交易签名，网络传输，合约执行等流程的安全，使账本系统中的用户资产得到保护。

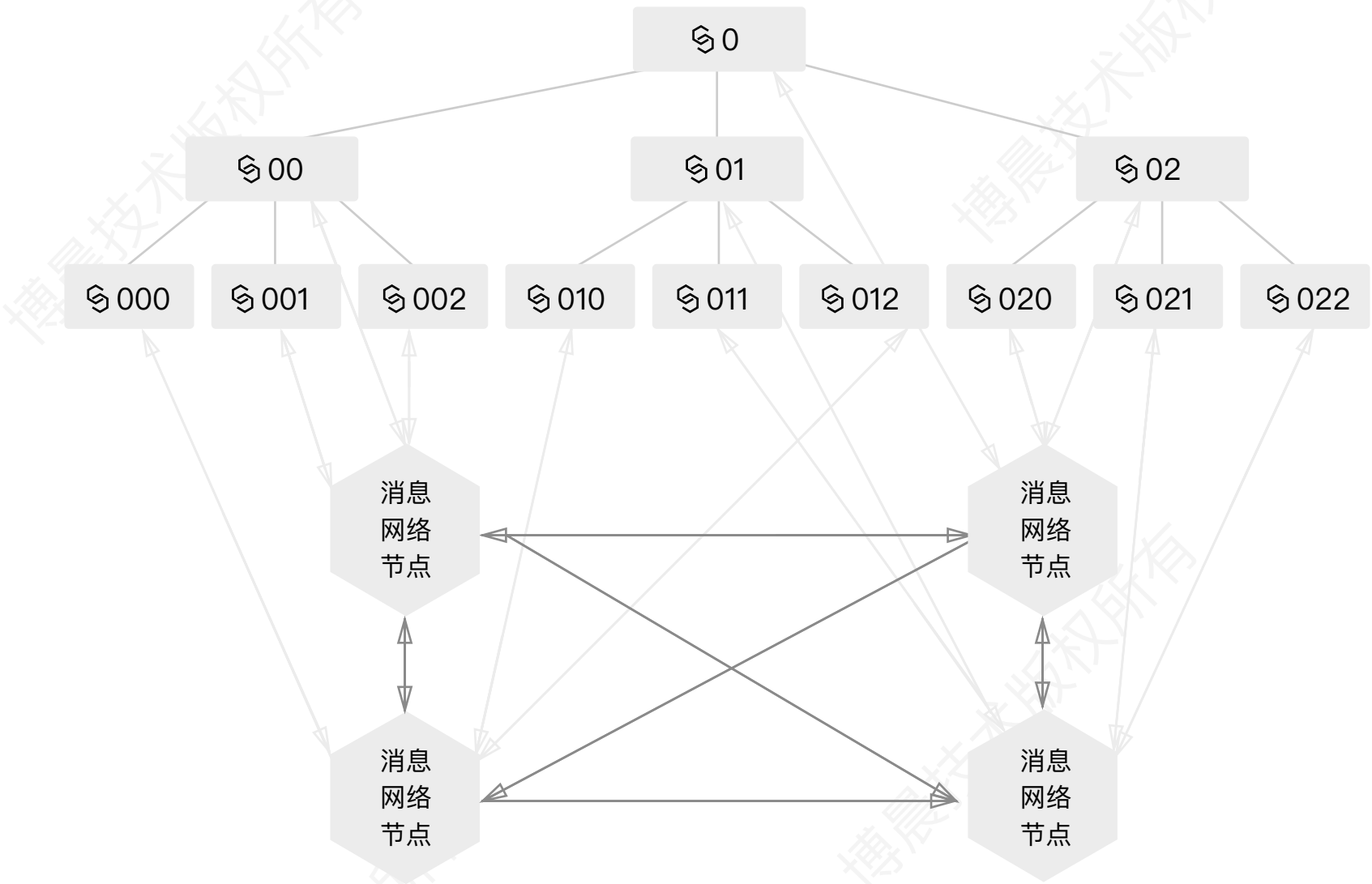
第二章 架构设计

2.1. 分布式账本

L0分布式账本系统由多个区块链以及消息网络组组成。

每个区块链根据其在网络中的层级位置有唯一的链编号ChainID ，最顶层的ChainID为0，下层的区块链ChainID前缀为其上层区块链的ChainID。每个区块链由若干区块链节点组成，每个节点用ChainID:PeerID来唯一标识其身份，每个区块链通过去中心化的协议维持自身的子账本。

下图是一个3层13个区块链加上拥有4个节点的消息网络组成的一个L0分布式账本。



图形代表区块链

对于某个子账本来说，如果交易双方都在同一个区块链（链A）内，则只在这个子账本记录这笔交易；如果交易双方在不同的区块链（链A和链B）上，则需要在区块链A和区块链B账本上同步记账。我们的跨链共识算法可以在A和B两个区块链都满足拜占庭容错的情况下，完成交易并同步记录在双方区块链的账本上。

通过这种层次化结构的设计，当多笔交易的参与方在不同的区块链上时，这些交易可以在多个链上并行执行。通过横向和纵向扩展分布式账本的区块链网络，整体交易性能可以同步提升。

为了解决区块链网络互通问题，保证跨链交易的消息可靠性，我们引入了消息网络。在整个分布式网络中，每个区块链节点仅和同区块链的其他节点建立直接的TCP连接，与其他链的节点通信则通过消息网络完成。每个区块链的节点加入消息网络后，整个消

息网络会对自己的区块链节点路由表进行相应的更新。区块链节点只需指定消息的目标区块链chainID或者目标区块链的特定节点chainID:peerID，并将该消息投递到区块链网络，消息网络就可以通过最短的路径将消息送达目的区块链节点。

2.2. 整体架构

对L0整体架构分为三层：核心层、服务层、应用层。

核心层由区块链节点和消息网络组成，提供账本的交易广播、共识计算、合约执行、身份认证、数据存储等功能。核心层可以通过弹性平滑扩展提升交易处理能力。企业可以快速部署自有的核心层，也可以接入基础平台供应商的核心层。

服务层可以承接分布式账本的各种业务场景，企业可以通过服务层构建相关的具体业务，包括在服务层构建和提交自己的智能合约，构建自己的资产体系，维护自己的业务数据、用户数据等。

应用层向终端用户提供基于分布式账本的应用服务，如各类型数字资产的钱包、交易应用等。用户通过应用层来管理资产或者进行交易。

第三章 底层设计

3.1. 账本数据

L0 的账本包括两部分数据，区块数据和状态数据。

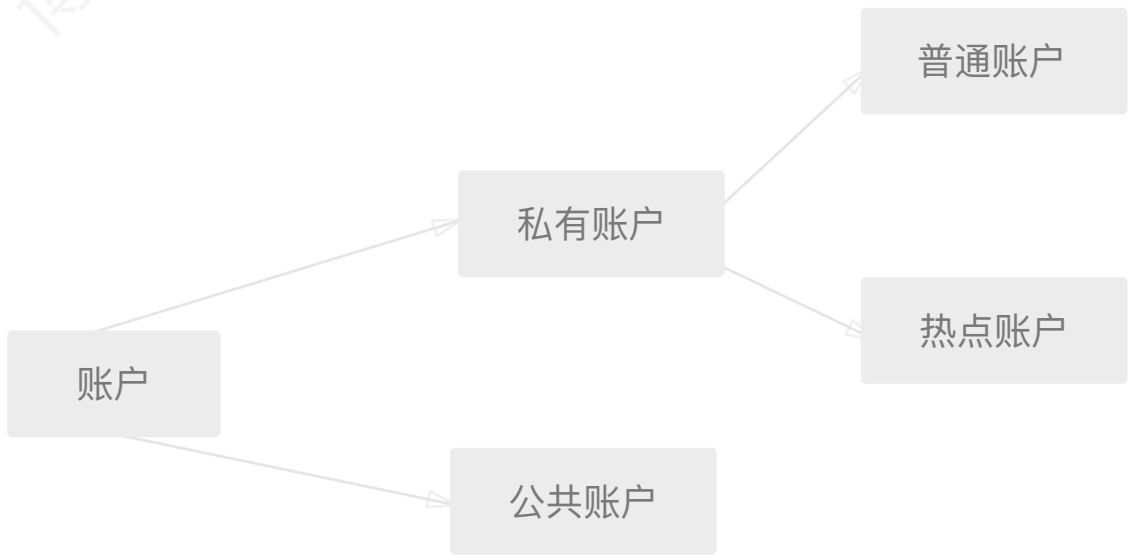
区块数据以链的形式存储在账本中，包括交易信息、状态数据hash、交易列表hash以及前一区块hash等内容。状态数据为(key,value)形式的数据对，所有的状态数据都由区块数据中的交易生成。状态数据只保存最新版本，不保存每个状态的历史数据。

系统启动时节点会对账本进行验证，计算状态数据hash值和区块的hash值，确保数据没有被篡改。

3.2. 账户

账户数据包含该账户的余额，账户类型，交易序号等其他数据。账户在账本中的存储数据称为账户状态，以(key,value)的形式存储在状态数据中。

L0中的账户类型如下图：



3.2.1. 私有账户(P)

私有账户中的资产有明确的所有者，所有者可以通过私钥或者合约代码使用该资产。通过私钥控制的账户，账户地址由公钥生成。该账户中的资产转出交易，必须使用相应私钥对交易进行签名，方可完成。合约代码控制的账户，向外转出资产由合约代码执行确认。

3.2.2. 普通账户(N)

位于分布式账本最底层的区块链上，以链C为例，账户拥有唯一的地址C:N。每发生一笔有效交易，C的账本上会纪录N的该笔交易以及账户状态等数据，如果是一笔跨链交易，另一个交易参与方不在C链(例如链D的账户M)，那么D的账本中会同步记录该笔交易，并更新M的账户数据。

系统启动时节点会对账本进行验证，计算状态数据hash值和区块的hash值，确保数据没有被篡改。

3.2.3. 热点账户(H)

热点账户H在多个层的多个链上拥有账户数据，这些账户由同一把私钥控制，账户资产为多个链上的资产总和。与普通账户不同，热点账户在多个链上的账户可以同时进行交易，不同链上的交易允许有相同的交易序号。

3.2.4. 公共账户(L)

每个区块链在其上层区块链中有一个对应的公共账户，公共账户的资产是其对应的下层区块链资产的汇总，没有具体的所有者，不能用来执行交易和支付操作。在上层区块

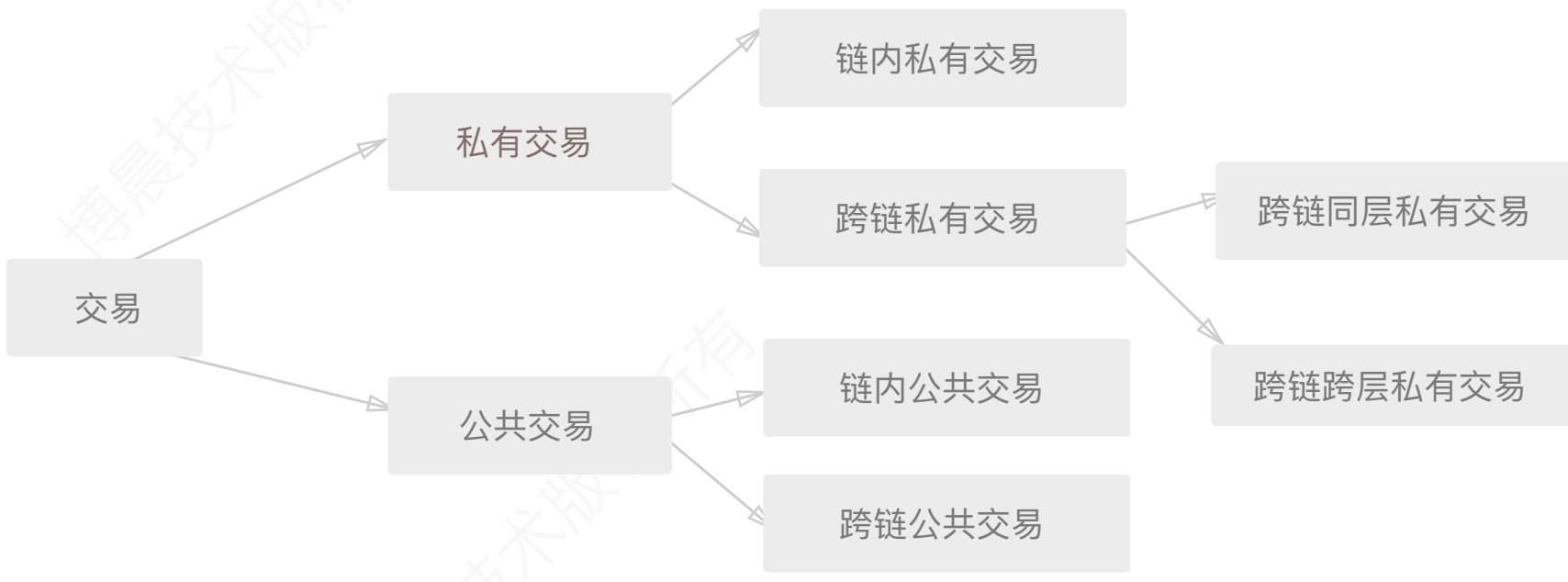
链的账本中，包含了下层区块链中所有交易汇总后的交易信息，交易可以反映下层区块链的交易金额和交易频次，并且可以用来确认整体账本的一致性。

3.3. 交易

L0目前支持两个参与方进行的资产转移交易，需要更多参与方或者更复杂转移方式的交易可以通过智能合约来完成。

一条典型的交易包括交易类型，付款方账户及所在链，收款方账户及所在链，交易金额，时间，签名等信息。

L0中的交易类型如下图：



3.3.1. 私有交易

由确定的所有者发起，可以是私钥持有者，也可以是合约。为了确保交易的安全，L0处理交易时，会对交易进行多个维度的验证。对于有私钥控制的付款账户，首先需要检查交易是否具备付款账户的正确签名；其次为了确保交易不会被恶意重复提交，一个账户提交的付款交易序号必须连续递增。

3.3.2. 公共交易

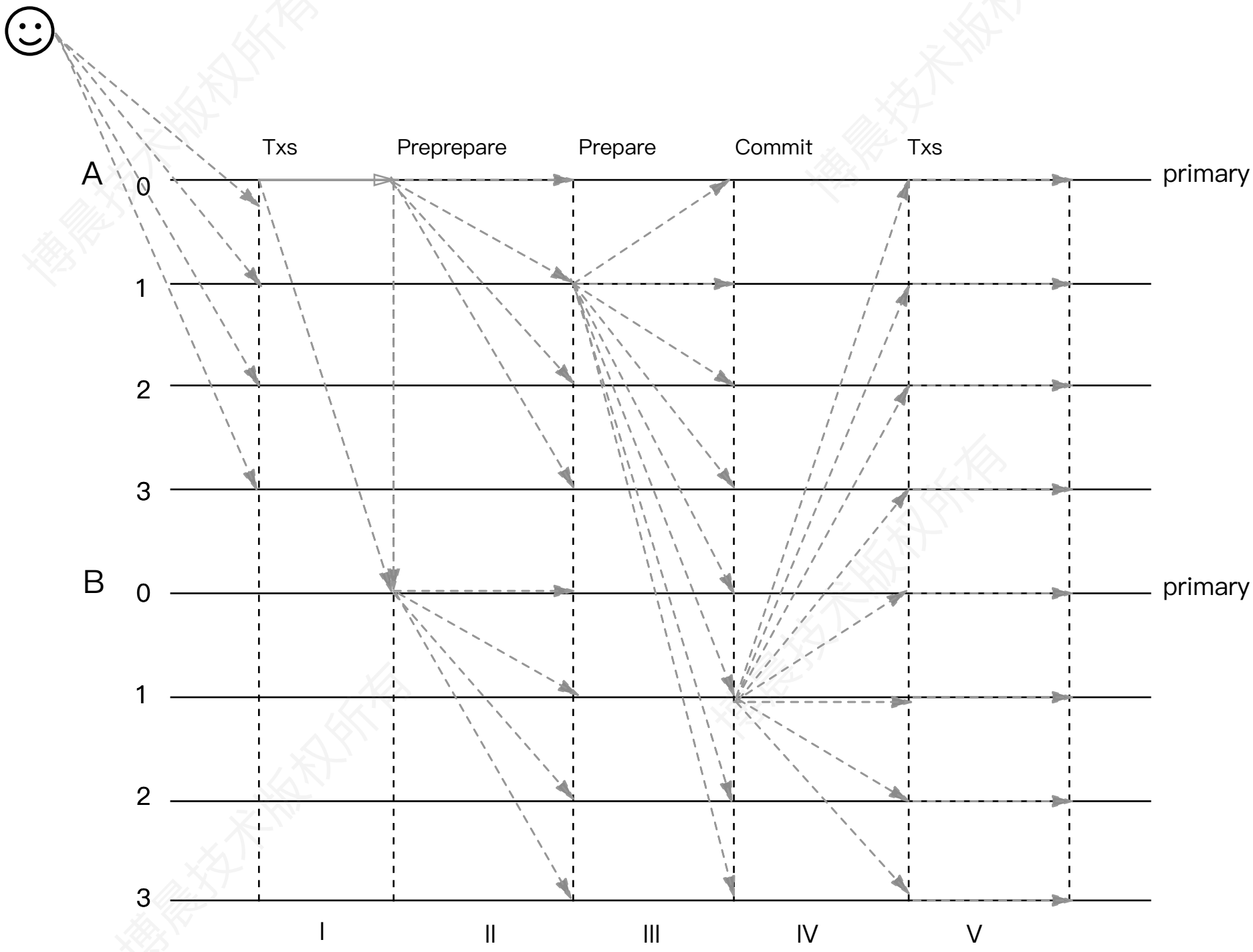
是一种基于层级的汇总交易，体现的是下一层级中，以区块链为单位（对应于上层的一个特定公共账户），链内与跨链交易的汇总合并。交易不由密钥控制，而是通过共识机制进行验证。所有的交易都会被逐层汇总上报，最终顶层账本可以查询到整个账本的所有交易汇总信息。

3.4. 共识算法

区块链常用的共识算法有pow，pos，raft，pbft，paxos等，其中pbft因为算法消耗小，性能高，且可容忍欺诈节点，被很多联盟链/私有链采用。

在L0中，两个区块链需要对同一笔交易达成共识并保证同步记帐，达成跨链共识是对共识算法的基本要求。L0采用的lbft共识算法是对pbft协议的改进，可以确保在容错范围内，每笔交易都在不同的参与方区块链上同步处理。

在lbft协议中，拥有3f+1个节点的A区块链和拥有3k+1个节点的B区块链进行跨链交易时，区块链A发起一笔到区块链B的交易，确认记账需要以下步骤：



1　A链主节点广播Preprepare交易到B链节点（主节点即共识消息发出节点）

2　A链和B链主节点分别广播Preprepare到各自链的从节点（从节点即共识消息投票节点）

3　A和B链的从节点分别对Preprepare的交易进行验证，验证通过后广播Prepare消息到A，B区块链的所有节点

4　A和B链的节点收到2f+1的A链节点以及2k+1的B链节点的相同Prepare消息后广播Commit消息到A，B区块链的所有节点

5　A和B链的节点收到2f+1的A链节点以及2k+1的B链节点的相同Commit消息后确认交易，该笔交易会记录在该节点账本上

在拥有3f+1(也适用于3f+2或3f+3)的L0区块链中， 具有f个节点的容错性能。

在错误节点数小于等于f时，错误节点不影响跨链双方诚实节点对交易的确认，跨链交易可以正常记账。

在错误节点数大于f小于2f+1时，诚实节点无法确认交易，跨链交易无法记账。

在错误节点数大于2f+1时，错误节点有联合作恶并对账本造成分叉的可能，可以造成跨链交易双方账本数据不一致，还可以操纵本地账本数据。

在错误节点数大于2f+1时，错误节点有联合作恶并对账本造成分叉的可能，可以造成跨链交易双方账本数据不一致，还可以操纵本地账本数据。

3.5. 智能合约

L0的普通交易只能满足有限的应用场景，除此之外，我们还提供了智能合约以满足更丰富的场景需求。通过智能合约的部署，执行和查询操作，可以很方便的实现基于UTXO的数字资产、多方参与的交易场景等包含复杂逻辑的合约应用。

L0的核心层为智能合约提供了模块化接口，这些接口可以对接不同的智能合约引擎，实现智能合约模块的可插拔，方便合约引擎的二次开发。接口包括数据接口(合约状态操作接口、账本查询接口、加解密相关等等)，引擎接口(合约部署、验证、执行等)，以及合约权限控制接口(合约创建条件、创建代价等)。

合约部署时，通过提交一条包含合约代码以及参数的合约交易到L0创建合约账户，并将合约代码储存在合约状态中，还需要制定合约引擎以及各项参数。合约执行时，提交合约执行的交易以及该交易包含合约执行的参数，L0调用合约引擎做出相应的操作，并通过数据接口更新账本数据。

我们会对L0的智能合约体系进行持续优化，也鼓励开发者根据自己的需求开发合约引擎。更详细信息请参考开发者文档。

第四章 模拟支付场景测试

4.1. 测试背景

为了验证L0 在高并发金融业务中的实际功能和性能表现，我们模拟了一个小额支付的测试场景。在典型的支付场景中，对TPS有很高的要求，例如，春节期间微信红包业务达到了峰值数十万笔的TPS。对传统区块链来说，这种要求是很大的挑战。L0在设计上可以支撑这类高并发业务，为了检验实际效果，我们进行了此次测试。

测试场景包含的账户类型：

普通账户

普通账户在树型分布式账本的一个子账本中存在，由用户持有私钥并控制账户，可以用来进行一对一的普通付款和收款操作。

热点账户

热点账户在树型分布式账本多个子账本中存在分账户，所有分账户由一把私钥控制，热点账户可以实现很高的收付款并发交易。

测试场景包含的交易类型：

单笔付款交易

付款方和收款方都是单一用户，且都是普通账户或者热点账户，用于普通的支付场景

批量付款交易

付款方为热点账户，批量向多个用户支付，例如发薪，发红包等场景

批量收款交易

收款方为热点账户，同时接收多个用户支付，例如比较大规模的商户收款操作

4.2. 测试方案

4.2.1. 账本规模

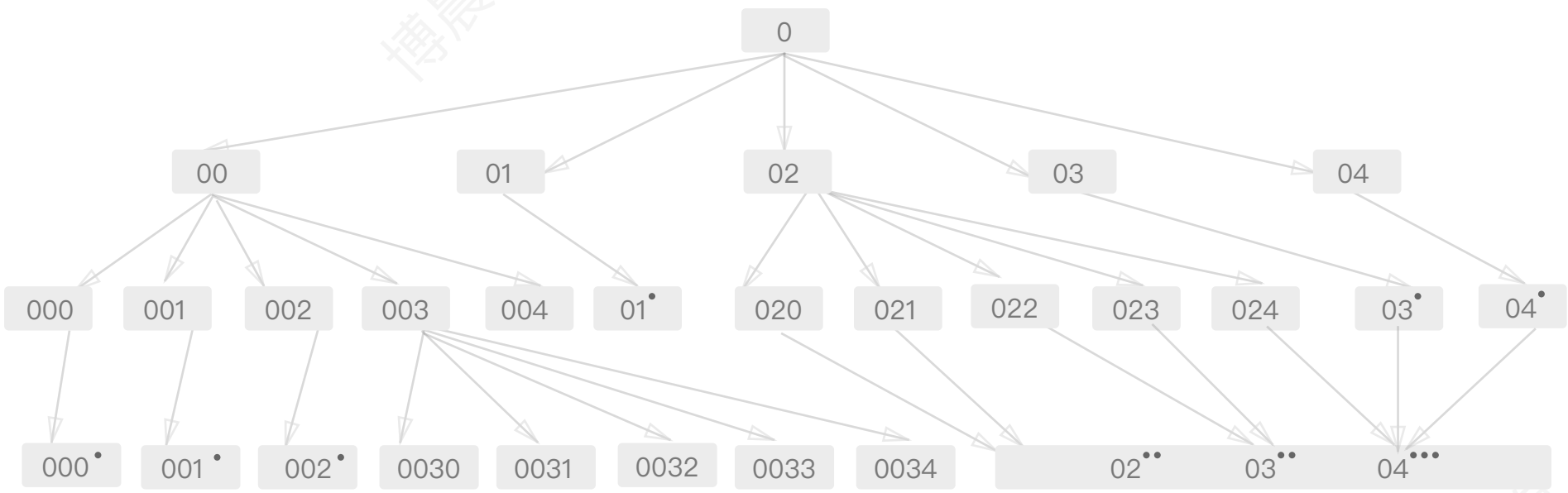
本次测试由测试程序、L0账本区块链网络和L0账本消息网络构成。

4.2.2. 测试程序

根据配置构造并提交海量的交易到服务层，本次测试采用一组测试程序发送不同的交易。可以根据配置发送不同TPS、不同构成的各种交易。

4.2.3. L0账本区块链网络

本次测试L0帐本区块链划分为4层, 每层分别拥有1,5,25,125共156个子帐本区块链。每个区块链由四个共识节点构成。



4.3. 测试环境

本次测试采用多虚拟机集群进行，服务器配置如下

4.3.1. 服务器配置

硬件配置	8核 / 32G内存
网卡	1000M/10000M
操作系统	Centos 7.0/Ubuntu 16.04
执行容器	虚拟机内直接运行　/ docker 容器内运行
gcc	5.3版本以上

4.3.2. 服务器规划

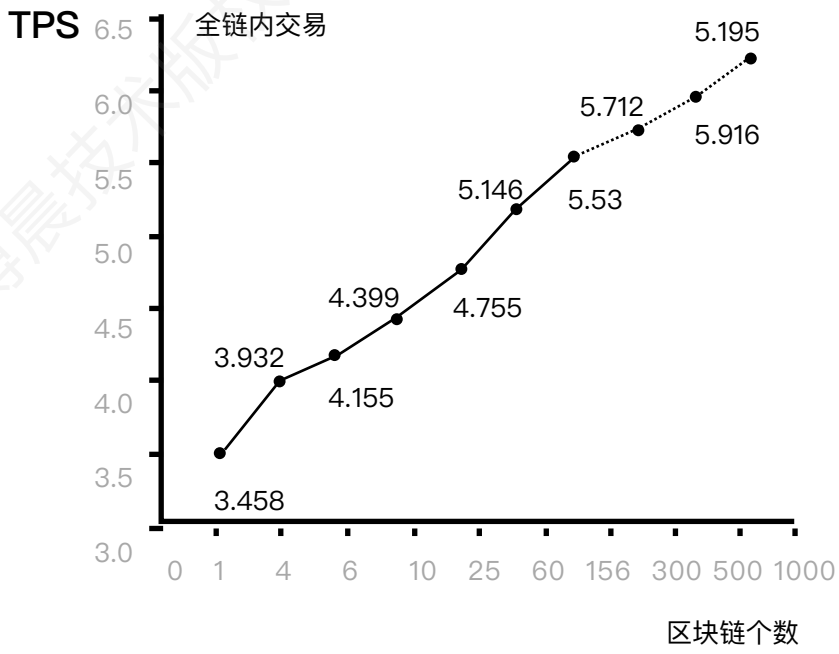
模块名称	占用服务器个数	每服务器运行实例数
运维平台	1	1
区块链共识节点	78	2*4
消息网络节点	13	2
测试程序	8	1

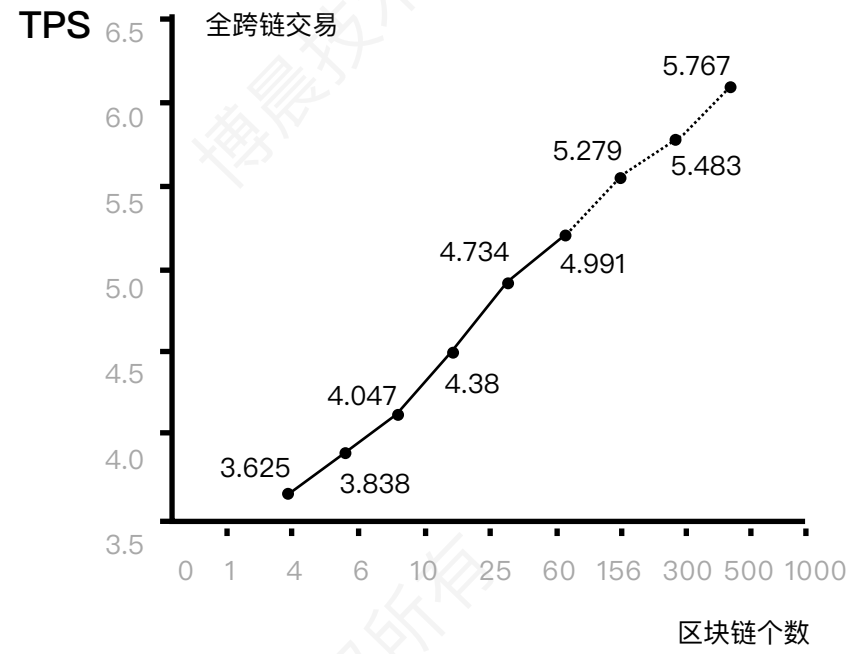
4.4. 测试结果

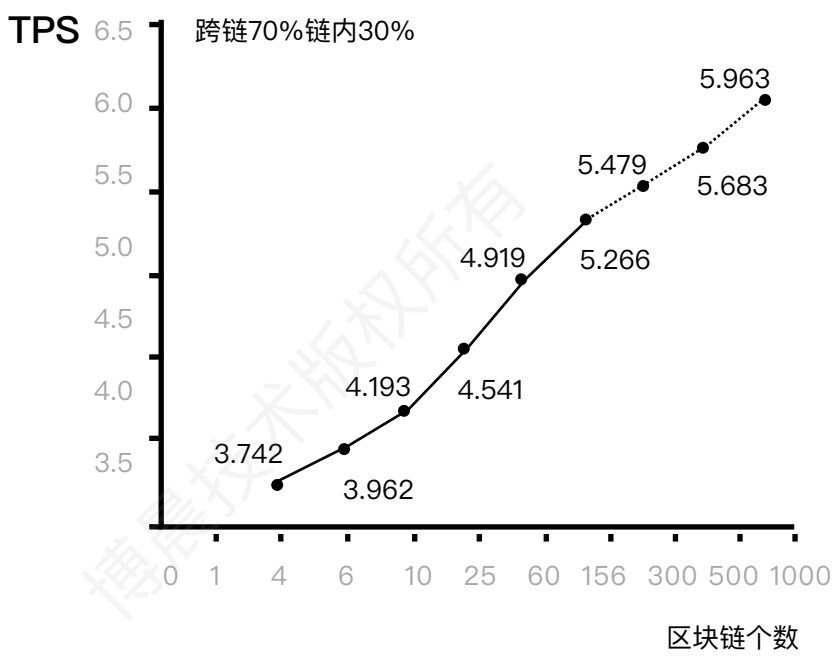
不同交易类型下账本总体性能(TPS):

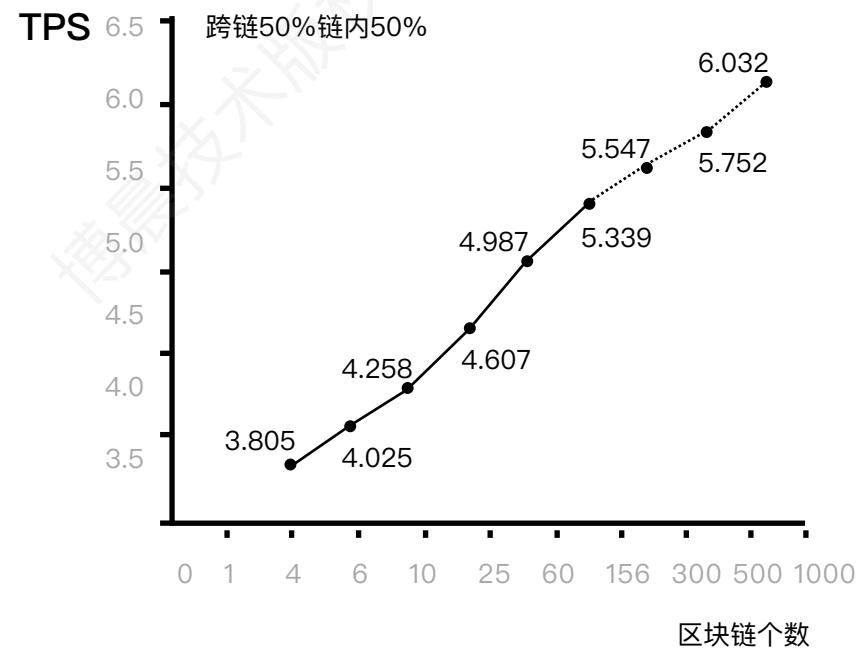
区块链个数	全链内交易	全跨链交易	跨链70% 链内30%	跨链50% 链内50%	链内70% 跨链30%
1	2873	NA	NA	NA	NA
4	8547	4214	5525	6380	7668
6	14289	6891	9161	10590	12758
10	25088	11137	15603	18112	22016
25	56923	23983	34760	40453	49439
60	139821	54219	83037	97020	119562
156	338938	97847	184498	218392	276395
300	515185	190212	301180	352698	436714
500	824297	304339	481888	564318	698743
1000	1566165	584331	918631	1075247	1330047

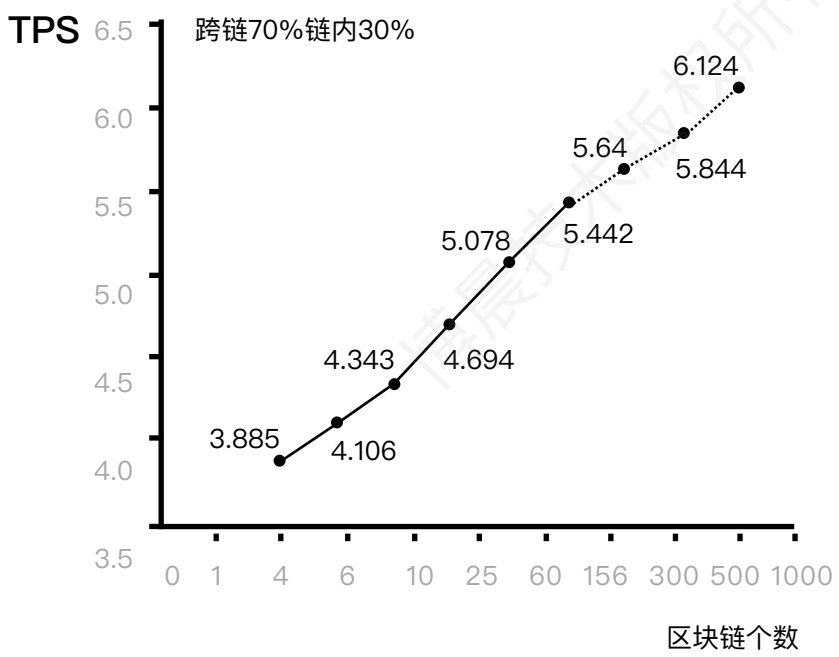
不同交易类型下账本总体性能（TPS）











* 纵坐标经过了1g10对数转换

* 每笔跨链交易会在两个区块链上记账，因此TPS计算跨链交易时，每个链交易乘以50%。

* 受限于测试环境,区块链个数300/500/1000为按模型预测值。