软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(9):4294−4309 [doi: 10.13328/j.cnki.jos.006651]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链星型分片架构通量模型及应用*

王柯元[1,2], 姜 鑫[1,2], 贾林鹏[1,2], 段田田[1,2], 孙 毅[1,2]

[1](中国科学院 计算技术研究所, 北京 100190)

[2](中国科学院大学 计算机科学与技术学院, 北京 100049)

通信作者: 孙毅, E-mail: sunyi@ict.ac.cn

摘 要: 并行化是区块链扩容方案中最有效的一类方案, 现有的并行化方案可根据网络架构分为星型架构与平行架构两类, 但是当前的研究工作中, 缺少对于星型分片架构方案的性能边界及性能瓶颈影响因素的分析. 因此, 针对不同的星型分片架构方案抽象出了一种通用的区块链星型分片架构, 并对该通用架构中的交易过程进行了量化建模, 得到了区块链通量与分片数量的关系, 建立了星型分片架构的通量模型. 根据建立的星型分片架构通量模型, 可以发现星型架构的通量性能存在上限, 存在一个最优的分片数量使得系统的通量达到最高, 且通量的最大值与主链功能复杂度存在明确的函数关系. 基于所提的通量模型, 相关的区块链系统可以结合自身方案的设计, 平衡分片数量与主链功能复杂度, 使得系统通量达到理论上限, 因此对于星型并行化方案设计具有重要指导意义.

关键词: 区块链; 并行化; 分片; 星型分片架构; 通量模型

中图法分类号: TP393

中文引用格式: 王柯元, 姜鑫, 贾林鹏, 段田田, 孙毅. 区块链星型分片架构通量模型及应用. 软件学报, 2023, 34(9): 4294–4309. http://www.jos.org.cn/1000-9825/6651.htm

英文引用格式: Wang KY, Jiang X, Jia LP, Duan TT, Sun Y. Throughput Model of Starlike Sharding Structure for Blockchains and Its Applications. Ruan Jian Xue Bao/Journal of Software, 2023, 34(9): 4294–4309 (in Chinese). http://www.jos.org.cn/1000-9825/6651.htm

Throughput Model of Starlike Sharding Structure for Blockchains and Its Applications

WANG Ke-Yuan[1,2], JIANG Xin[1,2], JIA Lin-Peng[1,2], DUAN Tian-Tian[1,2], SUN Yi[1,2]

[1](Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China)

[2](School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Parallelization is one of the most effective blockchain scalability solutions, and the existing parallelization schemes can be classified into two categories, i.e., starlike structure and parallel structure, according to the network structure. However, the current research lacks the analyses of factors affecting the performance boundary and performance bottleneck in starlike sharding structure. To address this problem, this study abstracts a general starlike sharding structure of blockchains for the schemes adopting different starlike sharding structure, and the transaction process in this general structure is quantitatively modeled to derive the relationship between throughput and the number of shards in starlike sharding structure. According to the constructed model, there exists a performance limit in starlike sharding structure and an optimal sharding quantity to maximize the system throughput. An explicit functional relationship exists between the maximal throughput and the functional complexity of the mainchain. With the proposed throughput model, related blockchain systems can balance the number of shards and the functional complexity of the mainchain to reach the theoretical upper limit of system throughput with the consideration of their specific design. Therefore, the work of this study has significant guiding value in the design of the schemes adopting starlike parallelization.

Key words: blockchain; parallelization; sharding; starlike sharding structure; throughput model

* 基金项目: 国家重点研发计划 (2019YFB1404903); 国家自然科学基金 (61972382, 61772502); 内蒙古自然科学基金 (2020MS06017)
收稿时间: 2020-11-05; 修改时间: 2021-06-03, 2021-12-13; 采用时间: 2022-01-18; jos 在线出版时间: 2023-02-08
CNKI 网络首发时间: 2023-02-08

区块链技术自 2008 年比特币[1]提出以来受到了广泛关注并逐渐挖掘出了强大的潜力. 最初区块链技术主要应用于数字货币领域, 后来向着更广阔的应用场景发展, 现在区块链技术已应用到诸多领域, 但是主要局限在版权保护与产品溯源的存证类应用和低频的数字资产交易场景中. 面对实时支付、物联网等高频交易场景, 区块链的通量严重不足, 无法满足现实需求, 这也限制了其应用领域的进一步扩展.

通量是衡量区块链系统性能的指标之一, 为单位时间内处理的交易量 (transactions per second, *TPS*), 它也是目前区块链的技术瓶颈. 当前主流的公有链系统如比特币、以太坊[2]的通量处于 10^1 量级, 联盟链系统超级账本[3,4]的通量处于 10^2 量级, 与 中心化的支付系统如 Visa、MasterCard 信用卡 10^3 以上的数量级和微信钱包与支付宝峰值时可以承载的 10^5 以上的数量级相差甚远. 区块链系统的交易处理速度都还远不及中心化系统, 在高并发交易的场景无法大规模投入使用. 因而, 提高区块链通量已经成为区块链技术突破的迫切需求.

解决区块链系统通量问题的方案之一是分片技术, 其通过提升交易处理的并发度, 来提高通量的数量级, 可以降低区块链网络的拥堵、减少交易成本、吸引更多用户、解决支付效率低下问题、提高存储空间的可扩展性, 以及催生去中心化应用的发展. 近年来, 国内外涌现了很多团队研究区块链系统的分片方案, 这些采用分片技术的区块链项目按照并行化架构可分为两种: 有主链作中转的星型架构 (Polkadot[5]、以太坊 2.0[6]、Zilliqa[7]等) 和片间直接交互的平行架构 (Omniledger[8]、Rapidchain[9]、Monoxide[10]、Chainspace[11]、Multivac[12] 等). 上述采用星型分片架构的项目中的通量性能分析着重于分片后各分片片内交易处理速度的线性叠加, 而缺少对主链在跨片交易处理过程中通量上限的研究. 对此, 本研究抽象出一种通用的区块链星型分片架构, 进而分析推导星型分片架构中区块链通量与分片数量的关系, 从而得到通量模型, 并以以太坊 2.0 和 Polkadot 为例将其应用到现有的并行化场景当中.

本文的主要贡献如下.

1) 首次对国际上主流的区块链并行化方案及应用按照组织架构分成星型架构和平行架构两类, 针对不同的星型分片架构方案抽象出了一种通用的区块链星型分片架构, 并对该通用架构中的交易过程进行了量化建模.

2) 通过分析推导星型分片架构中区块链通量与分片数量的关系, 建立了星型分片架构的通量模型. 并根据该模型得出, 星型架构的通量性能存在上限, 存在一个最优的分片数量使得系统的通量达到最高, 且通量的最大值与主链功能复杂度存在明确的函数关系, 在使通量达到最大的分片数量临界值前, 通量呈线性稳定增加; 在临界值后, 通量会缓慢地下降, 且有下界.

3) 为采用星型分片架构的相关区块链项目提供分片数量与主链功能复杂度的参考, 将通量模型应用于现有并行化场景以太坊 2.0 和 Polkadot, 分析最优的片内交易与跨片交易的速度关系, 平衡分片数量与主链功能复杂度.

1 相关研究

1.1 区块链技术

区块链技术的概念起源于比特币. 2008 年, 一位自称中本聪 (Satoshi Nakamoto) 的神秘人在“密码朋克”组织 (Cypherpunk) 的加密邮件系统上发表论文《比特币: 一个点对点的电子现金系统》[1], 并于 2019 年正式上线比特币系统. 自此, 区块链受到了广泛关注并逐渐被挖掘出了强大的潜力. 其本质是由既有的技术或概念如分布式存储、P2P 通信、共识机制、密码学算法、智能合约等组合而成的新技术体系——去中心化的分布式账本. 区块链系统中的节点们可以不必相互信任便可以通过一套统一的共识机制共同维护一个最终一致性的账本. 从架构来看, 区块链是一种分布式、去中心化、具有强鲁棒性的计算与存储架构. 宏观上, 没有中心化机构控制, 网络中节点处于对等的关系, 协作完成交易的验证和存储, 分布式地共享相同的数据, 即账本; 微观上, 节点将交易等信息按序放入区块, 将区块有序地串联成链条, 利用共识机制和数字签名等技术保证区块和其中交易的合法性. 在区块链系统运行过程中, 每个节点共同组成一个 P2P 网络, 均要验证、执行、记录相同的交易, 没有一个中心化机构可以干预交易的执行顺序和结果. 区块间通过单向的哈希链条链接在一起, 任何对区块信息的改动都会导致颠覆所有的后续区块, 账本由所有节点共同维护增加了信息的透明性, 方便历史交易数据的追踪, 这样的组织设计为篡改数据带来

了极大的难度, 保证了整个区块链系统的安全. 区块链技术的出现首次解决了在无可信的中心化机构时, 如何建立多方在信息不对称情况下的共识, 形成一个多方参与、去中心或多中心的价值和信任网络. 区块链的应用场景有很多, 最初主要应用于数字货币领域, 后来向着更广阔的应用场景发展, 凡是涉及资金的金融领域, 涉及不可篡改需求的食品溯源、版权保护等, 涉及信息透明的教育、医疗、慈善等, 理论上都可以使用区块链技术解决问题[13]. 但是在实践当中区块链尚局限于存证类应用和低频的数字资产交易场景中. 面对实时支付、物联网等高频交易场景, 区块链的通量严重不足, 无法满足现实需求, 这也限制了其应用领域的进一步扩展, 与设想中价值互联网还有很长的路要走.

1.2 性能瓶颈

时至今日, 区块链仍然存在性能不足的问题, 这是致使其无法支撑起大规模应用的直接原因. 区块链的性能指标主要是通量和时延两个方面. 通量表示在固定时间内可以处理的交易数, 时延则表示对交易的响应和处理时间. 在实际的应用当中, 需要综合两个要素对项目进行研究. 只考虑通量而忽略时延会存在问题, 例如, 长时间的交易响应会阻碍用户的使用从而影响用户体验; 只考虑时延忽略通量则会造成大量的交易排队, 如果一些交易平台必须要满足处理大量的并发用户交易, 那么通量低的方案会被直接抛弃.

1) 通量

通量是单位时间内处理的交易量, 也是目前区块链亟待攻克的技术瓶颈. 当前主流的公有链系统如比特币、以太坊, 甚至联盟链系统如超级账本的通量均达不到高并发场景的基本使用需求, 与中心化的支付系统如信用卡、微信钱包和支付宝的处理能力相去甚远. 因而, 提高区块链通量已经成为区块链技术突破的迫切需求.

通量直接受制于区块链的可扩展性. 区块链领域的突破性建设受制于一个被广泛认可的理论“不可能三角”[14], 即安全性、去中心化和可扩展性三者不可兼得. 比特币与现阶段的以太坊采用的区块链技术便是一种追求去中心化与安全的技术组合, 每一个全节点都验证存储所有的交易, 使网络节点具有平等地位民主自治, 但也同时带来了巨大的校验成本和存储开销, 牺牲了可扩展性, 严重影响性能, 无法承载全球货币市场的支付需求.

从共识机制入手, 在确保安全性的条件下, 采用权益证明 (proof of stake, PoS)[15]、委托权益证明 (delegated proof of stake, DPoS)[16]等共识机制可以解决比特币工作量证明 (proof of work, PoW) 共识性能低的问题. 例如, 为了提升性能保证业务的开展, 从公有链衍生出了联盟链和私有链技术. 联盟链节点的加入需要申请和身份验证, 网络节点有一定的分工, 由部分节点来负责全局的共识, 但这种区块链技术实质上都是将去中心化进行多中心化的妥协. 而私有链已经成为了完全中心化的技术, 仅是一种自动化数据备份的方式.

从存储分片入手, 现在公有链的全节点虽然是去中心化分布式存储, 但每个全节点存储的是交易记录的全集, 导致每个全节点承载了巨大的存储和通信压力. 分片技术类似于同构的半独立多链, 共享全局世界状态, 但分开了交易历史的存储, 同时也将算力分散到了各个分片, 实际上是尽量保证去中心化的同时提升了可扩展性, 但牺牲了部分安全. 一个好的分片技术协议应该只需要在去中心化和安全性上做出极小的牺牲.

2) 时延

区块链交易存在较大的延迟. 在使用比特币进行支付时, 一般需要 10 min 来完成一次支付的确认, 若要保证支付的不可逆转, 则又需要等待连续的 6 个区块被完全确认, 这通常需要接近 1 h 的时间. 而目前常用的银行或第三方支付则都是秒级的, 相比之下, 区块链系统的支付效率可谓低下.

区块链的时延确认时间与中心化的交易系统不同的是: 中心化交易系统的时延仅仅是交易发送到服务器, 在服务器端进行确认, 再将交易成功与否的结果返回给用户的过程, 这 3 个步骤结束后交易确认就已经结束. 而相比于中心化系统, 有以下几个原因会使区块链系统的交易时延变长.

① 采用 PoW 共识算法的区块链, 需要庞大的计算找到正确的哈希值, 才可以获得本轮打包区块的记账权, 因此会有一定的出块时间. 同时较长出块时间也能保证区块链的分叉得以减少.

② 分布式的节点只认可最长的链作为主链, 以达成共识, 所以交易所在的区块只有获得了一定的认可后, 交易才能算作被确认.

③ 每一个区块可记录的交易数量有限, 即有一个容量上限, 这是由于网络节点里的所有节点都要同步数据、验证数据, 块的容量太大, 不利于传输, 验证也会造成一定的延迟, 会导致一些安全问题, 所以区块容量受制于网络传输速度和验证处理速度.

随着区块链技术的不断进步, 时延问题得到进一步的解决, 区块链处理交易的方式便会更大限度减少人工成本、提高效率.

1.3 扩容方案

目前为了解决公有链的可扩展性问题, 研究与开发人员提出了多种扩容方案, 如表 1, 可以总体上归类为链上扩容和链下扩容, 它们都可以达到提高交易处理能力的目的. 链上扩容指直接发生在区块链上, 通过改变区块链的基础规则, 如区块大小、共识规则等, 从而达到提高处理交易能力的解决方案. 而链下扩容则不直接改动区块链本身的规则, 而是在其之上再架设一层网络, 只将必要信息或需要共识参与时才与区块链进行信息交互和传播. 其本质上没有发生在区块链上, 因此这类方案被称为链下扩容, 也常被称作 Layer-2 扩容方案.

表 1 扩容方案概述

类型	方案	概述
链上扩容	区块大小扩容[17]	实践中, 单纯增加区块大小会威胁区块链的安全模型, 比特币中, 区块变大, 全网最后一个节点收到区块的时间也就越长, 恶意节点掌握足够算力更容易恶意分叉
	提高区块生成频率[18]	增加区块生成频率会加大分叉的概率, 造成计算资源的浪费, 有效哈希计算比降低, 降低网络的安全性. 同时节点之间的通信更加频繁, 增加了对网络带宽的需求
	隔离见证[19]	比特币中将数据签名从交易中剥离出来, 使区块大小不变的情况下, 通过减少单笔交易的信息量, 来容纳更多的交易, 达到扩容加速的效果
	共识改进	继 PoW 共识算法后提出 PoS、DPoS 等共识算法, 在一定程度上提高了通量, 但对于安全性和去中心化是一种妥协, 目前缺少能够兼顾三难困境的共识算法
	DAG 技术[20]	依据交易前后的粘连关系将区块组织成有向无环图的技术, 与严格串行的区块链相比提高了交易处理的并发度, 但目前尚未得到安全和一致性的验证
	分片技术[21]	从每一笔交易都要每一个节点验证存储转变为由特定的分片中的节点来验证存储, 分片内串行执行每一笔交易, 分片间并行处理交易, 提高系统通量
链下扩容	闪电网络[22]	比特币中的链下支付通道在有频繁交易的节点之间, 以保证金的方式构建一个预付款的池, 不超过这个额度的交易不在主链区块里记录, 只有在结算的时候才发生一笔链上交易, 从而减轻小额交易对主网的压力
	雷电网络[23]	比特币闪电网络的以太坊版本, 为以太坊区块链在链下支付通道执行符合 ERC20 标准的代币传输
	侧链[24]	通过双向锚定技术使应用链数据和结算链数据无缝对接, 承上启下, 将应用数据均放在链下进行, 只有在结算时才在链上发起结算交易

最有效解决区块链扩容、提高系统通量问题的方案是采取链上并行化架构, 即分片技术. 按照区块链系统最初的设计, 网络中每个全节点都需要维护一份完整的区块链数据, 每个全节点需要验证所有的交易. 这虽然能够在一定程度上保证了区块链系统的安全性和稳定性, 但也无疑加重了系统的负荷, 其出块必须逐一处理的串行结构本身拖慢了交易处理的速度. 这就像车辆在单车道驾驶, 受制于道路难拓, 一旦车辆增多, 无论车速多快, 最终都会产生拥堵. 而且当前公有链随着时间的推移, 对全节点的存储与性能要求越来越高, 全网能够满足条件的节点越来越少, 这与去中心化的初衷是相违背的. 对此, 应改变现有架构, 降低单个节点的工作量. 区块链技术社区寻求一种能够保证区块链安全性和稳定性的同时, 又能够提高区块链系统的处理交易速度的方式.

分片概念源于一种基于数据库分成若干片段的传统扩容技术[25,26], 利用分而治之的思想通过将数据库分割成多个碎片并将这些碎片放置在分布式网络中. 区块链中的分片技术则是由曾经的单链处理所有交易、每个网络节点验证记录所有交易的高负载, 转为由各个分片维护与各自相关的交易, 不同分片的网络节点可以并行处理交易, 增加交易处理和验证的并发度, 实现并行出块, 从而提升了整个区块链网络的通量数量级, 降低区块链网络的拥堵, 减少交易成本, 吸引更多用户, 解决支付效率低下问题, 提高存储空间的可扩展性, 以及催生去中心化应用的

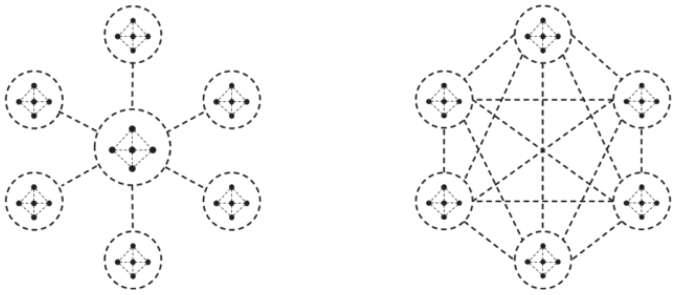
发展.

近年来, 国内外涌现了很多团队研究区块链系统的分片方案. 2016 年, Luu 等人[27]最先将数据库中的分片技术引入区块链中, 提出了一种面向公有链的安全分片协议 Elastico, 可提供近似线性的扩展性, 同时容忍 1/4 的恶意节点. 该团队于 2017 年, 提出基于 Elastico 的公有链 Zilliqa[7]. 2018 年, Kokoris-Kogias 等人[8]指出 Elastico 存在节点数量较少的分片具有高损害概率, 分片划分不具有强抗预测性, 不能保障跨分片交易的原子性, 验证节点频繁切换分片导致性能下降等问题, 提出了具有横向扩展交易处理能力的区块链 OmniLedger. 随后, Zamani 等人[9]指出 OmniLedger 同 Elastico 一样只能容忍 1/4 的恶意节点, 共识过程中节点之间通信复杂度较高, 额外需要一个可信初始化过程来产生随机参数, 因此, 提出了一种拜占庭容错的公有链 RapidChain, 提升区块链的安全性和可扩展性. 2018 年, Vitalik 提出了一种基于双层设计的以太坊分片方案[6], 将以太坊区块链分为主链和分片链, 其中主链通过验证管理合约来管理分片链, 分片链采用 PoS 共识机制打包交易数据生成验证块, 通过这些验证块最终生成主链上的区块. 2019 年, Wang 等人[10]提出了水平扩展的扩容方案 Monoxide, 其中最终原子以及连弩挖矿两个创新号称同时满足区块链的安全性、去中心化和可扩展性这 3 项需求. Monoxide 将系统的节点划分到不同的异步共识组中, 跨片交易通过一种接力的方式完成, 保证整个过程最终会达成一个一致状态. 2020 年, Gavin Wood 针对链间交互需求提出的 Polkadot 项目[5]的主网上线, 其中继链-平行链架构将平行链的共识交给中继链来做, 共享安全模型, 每条平行链可以看作一条自成生态的公链, 也可以看作 Polkadot 网络的一个分片链. 平行链功能将于 2021 年上线, 届时平行链会逐个接入中继链网络.

2 抽象化星型分片架构

2.1 星型架构与平行架构

通过研究现有的并行化架构区块链项目, 按照网络架构, 可以将它们分为两大类: 星型架构和平行架构. 星型架构与平行架构的示意图如图 1 所示.



(a) 星型架构 (b) 平行架构

图 1 区块链并行化架构

星型架构是一种主链-分片链架构, 主链负责交易的最终确认和为系统提供安全保障, 分片链需维护并同步主链与本分片的数据. 片内交易可直接经过片内共识完成, 在一些项目中需要定期将状态锚定在主链[5,6]; 跨片交易则可以分为 3 个阶段: 发送方分片内共识、交易和相关证明在主链共识、在目的方分片共识. 该架构的通信与存储开销相对较小, 但随着跨片交易量的增加, 主链可能会出现“过载”的问题, 制约系统的性能.

平行架构是一种无需主链的架构, 片内交易可直接经过片内共识完成; 跨片交易在分片链间直接交互, 各分片维护并更新自身状态, 并分别与跨片交易的相关分片建立联系, 由客户端[8]或某一分片[9]保障跨片交易的原子性和分片间一致性. 该架构的通信与存储开销较大, 并且需要设计周密的共识机制来保证各分片的安全性.

2.2 星型分片架构

星型分片架构的区块链系统具有一些共同的功能特点: (1) 能够将交易进行分片存储, 不同分片的网络节点负责特定一部分交易的处理, 从而减少每个网络节点的压力. (2) 分片内节点之间的交易实现自治, 跨片交易通过一

个中间网络来传递, 即主链. 主链的具体功能视项目需求而定, 其基础功能是交易的路由转发.

针对上述基本功能特点, 本文抽象出一种通用的区块链星型分片架构, 如图 2 所示.

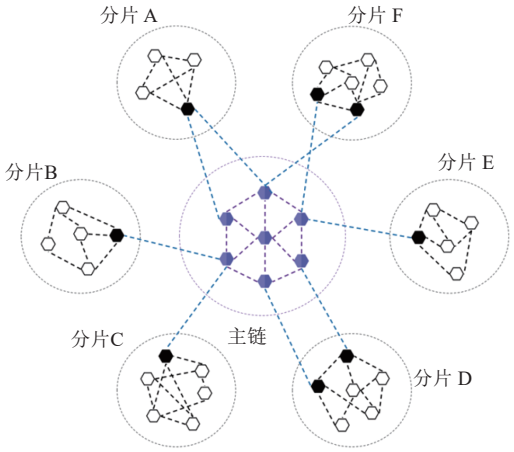


图 2　通用的区块链星型分片架构模型

在抽象出的星型分片架构中, 区块链由一条主链与不同分片对应的子链组成. 主链负责交易的最终确认和为系统提供安全保障, 分片链需维护并同步主链与本分片的数据. 每个分片维护与本分片相关的交易记录及账户状态. 每笔交易产生后, 会被送往对应的分片进行验证、执行并打包. 每个分片要处理两种交易: 片内交易和跨片交易. 片内交易顾名思义是隶属于一个分片内的两个账户之间的交易, 只在对应分片内进行处理; 而跨片交易, 是隶属于多个分片的账户之间进行的交易, 需要多个分片合作.

以分片 A 的账户 a 要向分片 B 的账户 b 发送一笔交易 tx 为例, 该笔交易属于分片 A 的跨片交易. 跨片交易具体过程如下.

① 交易 tx 被广播至分片 A , 通过分片 A 验证后更新账户 a 的相关状态, 并生成相关交易证明材料 m.

② 分片 A 将交易 tx 以及相关交易证明材料 m 发往主链, 主链的基本路由功能将其转发到分片 B 中.

③ 分片 B 根据相关交易证明材料 m 验证交易 tx, 交易 tx 通过验证后, 分片 B 更新账户 b 的状态. 至此, 跨片交易 tx 正式处理完成.

区块链的通量为单位时间内处理的交易量, X_{tx} 为一段时间产生的交易数量, t_{tx} 为这段时间产生的交易处理所需要的时间, 则通量的表达式为:

$$TPS = \frac{X_{\text{tx}}}{t_{\text{tx}}} \tag{1}$$

该架构需对交易过程涉及的诸多变量做出以下定义.

当区块链系统被划分为 N 个分片时, 每产生一笔交易, 该交易属于 i 分片的概率是 $\theta(i)$; 每产生一笔交易, 该交易属于 i 分片, 且交易的目的账户属于 j 分片的概率是 $\varepsilon(j,i)$, 则有:

$$\theta(i) = P(s_{\text{ID}} = i),\ i = 1,2,\ldots,N,\ \sum_{i=1}^{N}\theta(i) = 1 \tag{2}$$

$$\varepsilon(j,i) = P(r_{\text{ID}} = j | s_{\text{ID}} = i),\ i = 1,2,\ldots,N;\ j = 1,2,\ldots,N,\ \sum_{j=1}^{N}\varepsilon(j,i) = 1 \tag{3}$$

其中, s_{ID} 是一笔交易的发送方账户所在的分片; r_{ID} 是一笔交易的接收方账户所在的分片.

假设一较长时间段内产生 M 个交易, 并且它们服从概率分布 θ, 分配到不同的分片中, 第 i 个分片产生的交易数量为 $M\theta(i)$. 每一个分片内要处理 3 种交易.

① 片内交易, 每笔交易的处理时间为 t.

② 交易发送方账户在该分片的跨片交易, 每笔该种交易的处理时间为 αt.

③ 交易接收方账户在该分片的跨片交易, 每笔该种交易的处理时间为 βt.

主链的基本功能是用于实现跨片交易的路由转发. 主链与各分片是并行处理的; 主链上的交易是串行处理的, 每笔交易的处理时间为 γt.

分片方式的分类亦有按照网络分片、交易分片和状态分片的分类方式, 本文抽象出的星型架构性能模型也非针对网络分片、交易分片、状态分片中的某一个, 而是为了涵盖采用星型架构分片的普遍情况.

对于网络分片而言, 是将共识节点随机划分分片, 片内节点自行共识并将交易进行确认. 仅满足网络分片而不要求状态分片的星型分片架构系统如 Zilliqa 对主链的功能要求较低其主链仅做汇总各片共识的交易上链并产生随机数供下一轮分片, 也就是后文提到的主链功能复杂度较低, 这使得主链对交易处理的速度较快, γ 与 α 和 β 的数量级差较大.

在网络分片后不同分片会处理不同的交易, 按照什么规则将不同的交易分配给不同的分片是交易分片关注的问题, 例如按照发送方地址分片还是按照交易哈希分片等. 它解决了如何将一个交易分配到某个分片的问题, 并不会对抽象星型分片架构模型构成影响.

状态分片是当今业界最关注的分片方案, 它需要在前两者的基础上做到不同的分片存储不同的状态, 在采用星型分片架构的方案中, 以太坊 2.0 和 Polkadot 都致力于做到状态分片. 它们的共同特点是, 分片维护片内的状态, 隔一段时间将状态上传锚定至主链, 作为跨片交易获取状态的依据. 这类分片对主链的功能要求较高, 其主链功能复杂度较高, 主链处理交易的速度较慢, γ 与 α 和 β 的数量级差较小.

3 星型分片架构通量模型

3.1 主链性能与分片数量关系分析

星型架构采用主链-分片链架构, 主链的基本功能是能为跨片交易路由转发. 这种架构下, 随着分片数量的增加, 跨片交易的比重相应增加, 主链可能会出现“过载”的问题, 制约网络的性能. 在极限概念的分析下, 若区块链系统仅有一个分片 (也就是最初不分片的情况), 系统中不存在跨片交易, 没有采用并行化架构, 交易完全串行处理, 区块链的通量依然不足; 若区块链系统中每一个主链外的网络节点自成一分片, 系统中所有的交易均为跨片交易, 所有的交易均通过主链转发, 而主链上的交易依然是串行执行, 因此该情况的性能也类似于不分片的区块链系统, 通量依然不足.

经过上述理论分析, 随着分片数量的增加, 星型分片架构下的区块链系统的通量应该呈先增加后降低的趋势. 分片后的区块链系统会出现 2 种情况.

第 1 种情况: 如图 3 所示, 分片数量较少时, 在主链上路由转发等所消耗的时间远小于各分片交易处理时间, 因此该 M 笔交易处理完成的时间即为耗时最长的分片处理交易所需要的时间.

每一个分片的交易处理时间 t_{shard} 可表示为:

$$t_{\text{shard}} = t_{\text{intra-tx}} + t_{\text{inter-txA}} + t_{\text{inter-txB}} \tag{4}$$

其中, $t_{\text{intra-tx}}$ 为片内交易的时间; $t_{\text{inter-txA}}$ 为交易发送方账户在该分片的跨片交易; $t_{\text{inter-txB}}$ 为交易接收方账户在该分片的跨片交易.

$$\begin{cases} t_{\text{intra-tx}} = M\theta(i)\varepsilon(i,i)t \\ t_{\text{inter-txA}} = M\theta(i)[1-\varepsilon(i,i)]\alpha t \\ t_{\text{inter-txB}} = \sum\limits_{j\neq i} M\theta(j)\varepsilon(i,j)\beta t \end{cases} \tag{5}$$

将各交易处理时间表达式公式 (5) 代入公式 (4) 中, 第 i 个分片的交易处理时间 t_i 为:

$$t_i = M\theta(i)\varepsilon(i,i)t + M\theta(i)[1-\varepsilon(i,i)]\alpha t + \sum_{j\neq i} M\theta(j)\varepsilon(i,j)\beta t \tag{6}$$

则单位时间内处理交易的通量为:

$$TPS = \frac{M}{\max(t_i)} = \frac{1}{\max\{\theta(i)\varepsilon(i,i)t + \theta(i)[1-\varepsilon(i,i)]\alpha t + \sum_{j\neq i}\theta(j)\varepsilon(i,j)\beta t\}} \tag{7}$$

第 2 种情况: 如图 4 所示, 分片数量较多时, 在主链上处理交易路由转发等功能的时间已经超出每个分片处理交易所需的时间. 因此要等待主链上的所有跨片交易处理完成后, 其他分片才能够处理完成所有涉及本分片的跨片交易.

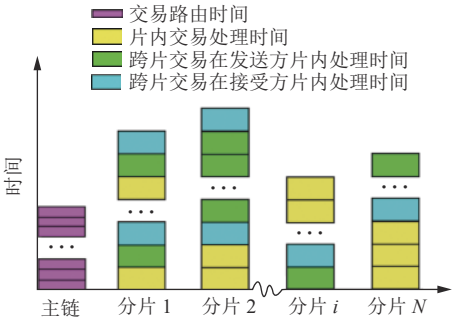


图 3 分片数量较少时各链交易处理时间

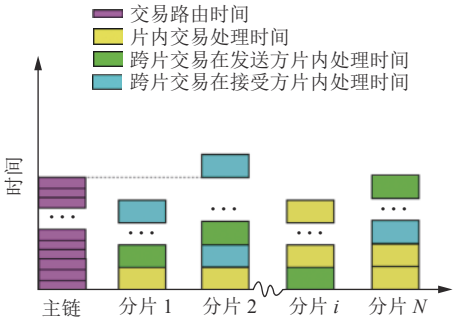


图 4 分片数量较多时各链交易处理时间

当分片数量较大后, 主链的交易处理时间成为系统瓶颈. 在一段较长时间内, 交易数量 M 较大, 单笔交易所耗时间可以忽略不计, 忽略系统处理的最后一个跨片交易在接收方分片的处理时间, 则可以看作区块链系统交易处理总时间 t_{total} 恒等于主链处理交易的时间 $t_{\text{mainchain}}$.

$$t_{\text{total}} \equiv t_{\text{mainchain}} \tag{8}$$

$$t_{\text{mainchain}} = M\left[1 - \sum_{i=1}^{N}\theta(i)\varepsilon(i,i)\right]\gamma t \tag{9}$$

$$TPS = \frac{M}{t_{\text{mainchain}}} = \frac{M}{M\left[1 - \sum_{i=1}^{N}\theta(i)\varepsilon(i,i)\right]\gamma t} \tag{10}$$

公式 (10) 中, 随着分片数量的增加, 片内交易比例降低、跨片交易比例增加, 分母会逐渐变大, 因此当主链交易处理时间已经开始超出各分片处理交易的时间时, 分片数量 N 的增加反而会降低区块链系统的通量.

综上, 通过两种情况的分析, 整体来看证实了先前通量随着分片数量 N 的增加, 是先增加到一个极限值后再逐渐减小的理论假设.

由此得到星型分片架构通用的通量性能模型: 当 $t_i > t_{\text{mainchain}}$ 时, 星型分片架构区块链的通量由最慢的分片链的速度制约; 当 $t_i \leqslant t_{\text{mainchain}}$ 时, 星型分片架构区块链的通量由主链的速度决定.

随着分片数量 N 的增加, 通量先是随之增加, 当分片数量 N 达到一个特定值后, 使 $t_i = t_{\text{mainchain}}$ (代入公式 (6)、公式 (9) 得到公式 (11)), 主链的处理速度刚刚达到瓶颈, 此后再增加分片数量 N 会使通量不增反减. 因此, 此时区块链系统的通量达到最大, 当前的分片数量 N 便是最佳的分片数量.

$$\max_i\left\{M\theta(i)\varepsilon(i,i)t + M\theta(i)[1-\varepsilon(i,i)]\alpha t + \sum_{j\neq i}M\theta(j)\varepsilon(i,j)\beta t\right\} = M[1 - \sum_{i=1}^{N}\theta(i)\varepsilon(i,i)]\gamma t \tag{11}$$

3.2 通量与分片数量关系计算

分片数量 N 是影响交易属于分片的概率分布 $\theta(i)$, 片内交易的概率分布 $\varepsilon(i,i)$ 和跨片交易的概率分布 $\varepsilon(j,i)$ 的重要因素, 因此引入它们以分片数量 N 为自变量的表达方式:

$$\theta(i) = f(N) \tag{12}$$

$$\varepsilon(i,i) = g(N) \tag{13}$$

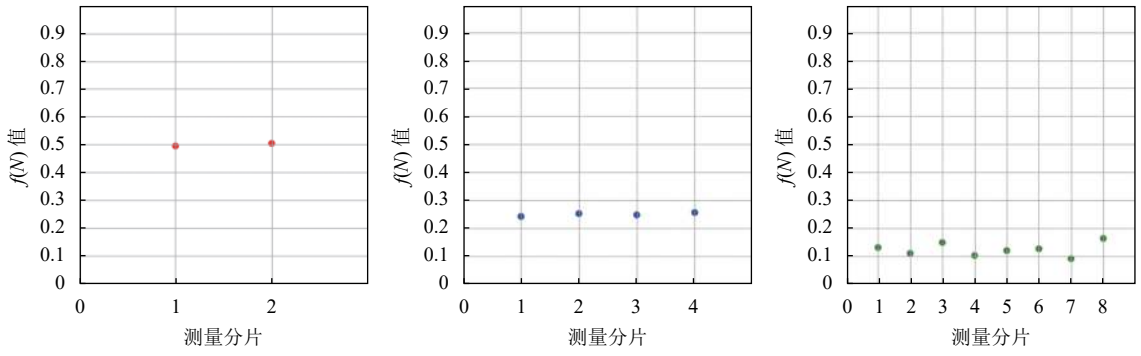
$$\varepsilon(j,i)=\frac{1-g(N)}{N-1},\ j\neq i \tag{14}$$

将公式 (11) 中的概率分布$\theta(i)$、$\varepsilon(i,i)$和$\varepsilon(j,i)$以分片数量N为自变量的表达方式代入, 得到主链处理速度刚好达到瓶颈时刻的分片数量N与网络交易处理时间参数的关系公式 (15):

$$\max_i\left\{f_i(N)g(N)+f_i(N)[1-g(N)]\alpha+\sum_{j\neq i}f_j(N)\frac{1-g(N)}{N-1}\beta\right\}=[1-g(N)]\gamma \tag{15}$$

3.2.1 普遍的均匀分片规则

在该星型分片架构通量模型中采用广泛使用的按照地址头部分片规则, 由于账户地址是随机生成的, 账户地址服从均匀分布, 每生成一笔交易, 其发送方地址会等可能地落在每个分片当中, 同时无论交易的发送方地址在哪一个分片, 交易的接收方地址也等可能地落在每一个分片中. 本文分析大量实际的交易数据验证交易属于分片的概率分布$f_i(N)$的值, 通过爬取以太坊浏览器 Etherscan 中最近的 30 万个区块中的交易数据, 计算得到在不同的分片数量N下对应的概率分布值$f_i(N)$近似$\frac{1}{N}$, 如图 5, 但由于存在一些较为热门的智能合约, 它们的合约地址发出的交易较为集中, 交易归属某分片的交易概率分布$f_i(N)$在$\frac{1}{N}$附近波动.



(a) 分片数量 N=2 (b) 分片数量 N=4 (c) 分片数量 N=8

图 5 根据以太坊历史交易数据模拟实验, 不同分片数量时各分片交易概率分布

公式 (12) 中交易归属分片的概率分布$f_i(N)$可视作:

$$\theta(i)=P(s_{\mathrm{ID}}=i)=f_i(N)=\frac{1}{N}(1+\sigma_i),\ i=1,2,\ldots,N;\ -1\leqslant\sigma_i\leqslant 1 \tag{16}$$

其中, 经过对历史交易数据模拟实验分成 2, 4, 8, 16, 32 片发现, 交易归属概率分布$f_i(N)$在$\frac{1}{N}$附近波动, 但概率不超过$\frac{2}{N}$, 而更高的分片数量模拟实验结果会因为统计数据不足逐渐失去统计意义, 因此可将σ上确界视为 1.

公式 (13) 中片内交易的概率分布$g(N)$的值可视作$\frac{1}{N}$:

$$\varepsilon(i,i)=P(r_{\mathrm{ID}}=i|s_{\mathrm{ID}}=i)=g(N)=\frac{1}{N},\ i=1,2,\ldots,N \tag{17}$$

公式 (14) 中跨片交易的概率分布可视作:

$$\varepsilon(j,i)=P(r_{\mathrm{ID}}=j|s_{\mathrm{ID}}=i)=\frac{1-g(N)}{N-1}=\frac{1}{N},\ j\neq i \tag{18}$$

公式 (11) 中为使等式成立, 等式左边应取最长的分片链处理交易时间, 对应公式 (15) 中则为选取$f_i(N)$最大的分片:

$$f_{\max}(N)=\frac{1}{N}(1+\sigma_{\max}),\ 0\leqslant\sigma_{\max}\leqslant 1 \tag{19}$$

将$f_{\max}(N)=\frac{1}{N}(1+\sigma_{\max})$, $g(N)=\frac{1}{N}$代入公式 (15) 通用的通量性能模型中化简得:

$$(1+\sigma_{\max})\left(\frac{1}{N^2}+\frac{N-1}{N^2}\alpha+\frac{N-1}{N^2}\beta\right)=\frac{N-1}{N}\gamma \tag{20}$$

变形为分片数量 N 的二次函数得:

$$N=\frac{(\alpha+\beta+\Gamma)+\sqrt{(\alpha+\beta+\Gamma)^2-4\Gamma(\alpha+\beta-1)}}{2\Gamma} \tag{21}$$

其中,

$$\Gamma=\frac{\gamma}{1+\sigma_{\max}} \tag{22}$$

公式 (21) 中得到的N值便是分片数量N的临界值, 即通量达到最大的最佳分片数量.

由此, 结合公式 (7)、公式 (10) 可以推导出在普遍的均匀分片规则下星型分片架构区块链的通量表达式为:

$$TPS=\begin{cases}\dfrac{1}{t}\cdot\dfrac{N^2}{(1+\sigma_{max})[1+(\alpha+\beta)(N-1)]}, & N<\dfrac{(\alpha+\beta+\Gamma)+\sqrt{(\alpha+\beta+\Gamma)^2-4\Gamma(\alpha+\beta-1)}}{2\Gamma}\\ \dfrac{1}{t}\cdot\dfrac{N}{\gamma(N-1)}, & N\geqslant\dfrac{(\alpha+\beta+\Gamma)+\sqrt{(\alpha+\beta+\Gamma)^2-4\Gamma(\alpha+\beta-1)}}{2\Gamma}\end{cases} \tag{23}$$

由公式 (23) 可知, TPS 与分片数量N的关系是分段函数, 曲线趋势应为: 开始时随着分片数量的增加, 通量随之线性增加. 当分片数量达到一个特定值时, 通量开始逐渐减少, 而非继续随之增加. t, αt, βt 均是一种在一个分片内的交易处理时间, 所以在此假设它们处于同一个数量级: $\alpha=1$, $\beta=1$. 但γ与α和β的数量级差是由主链在具体的功能实现中决定的. 不同的数量级差会导致不同的分片数量N的临界值, 即最优分片数量.

回到第 3.1 节中的极限思想, 若区块链系统仅有一个分片 (也就是最初不分片的情况), N 的值为 1, 小于临界值, 此时影响交易归属概率分布波动的参数$\sigma=0$, 将$\alpha=1$, $\beta=1$, $N=1$代入公式 (23) 的第 1 种情况, 计算得到通量 $TPS=\dfrac{1}{t}$; 若区块链系统中每一个主链外的网络节点自成一分片, 网络节点的数量就等于系统分片的数量N, 区块链作为分布式网络应用本就节点数量较多, 公式 (23) 的第 2 种情况下$\dfrac{N}{N-1}$的值可视作 1, 且这种极限情况下, 主链必须能够完成区块链系统的所有功能, 于是主链上单笔交易处理时间便等于普通区块链上一笔交易的处理时间, 即$\gamma t=t$, 代入公式 (23), 计算得到通量$TPS=\dfrac{1}{t}$. 两种极端情况, 利用推导出的星型分片架构区块链的通量表达式均能得到与不分片时的区块链相同的通量结果, 即$TPS=\dfrac{1}{t}$, 应验了先前极限概念的分析.

星型分片架构区块链中片内交易、发送跨片交易、接收跨片交易均是一个分片内对一笔交易的处理过程, 其广播、同步、验证等步骤相似, 可以合理地假设这 3 种交易的处理时间处于同一数量级, 即令 $\alpha=1$, $\beta=1$.

然而α, β与γ或Γ的数量级差要取决于主链的具体功能和具体实现. 例如, 如果主链仅实现最基本的路由转发功能, 则主链上每笔交易的处理时间γt就会很短, 仅取决于网络情况, γ大概在10^{-3}数量级左右[28], 但具体实现中难免会加入一些验证等保障安全的功能, 所以这个数量级要经过对具体系统测试才能得到准确的数值.

根据公式 (23) 的通量表达式, 不同的α, β, Γ会得出不同分片数量N的临界值. 因此在此列举当Γ的数量级分别为10^{-1}, 10^{-2}, 10^{-3}时, 星型分片架构区块链的通量增长倍数 (相比于不分片区块链系统的通量增长倍数) 与分片数量N的关系曲线.

当Γ与α和β的数量级差为10^1时, 通量增长倍数与分片数量关系曲线如图 6 所示, 此时使通量达到最高的最佳分片数量N为 32.

当Γ与α和β的数量级差为10^2时, 通量增长倍数与分片数量关系曲线如图 7 所示, 图 7(a) 中右侧平缓片段经过纵坐标拉伸得到图 7(b), 此时使通量达到最高的最佳分片数量为 256.

当Γ与α和β的数量级差为10^3时, 通量增长倍数与分片数量关系曲线如图 8 所示, 图 8(a) 中右侧平缓片段经过纵坐标拉伸得到图 8(b), 此时使通量达到最高的最佳分片数量为 2 048.

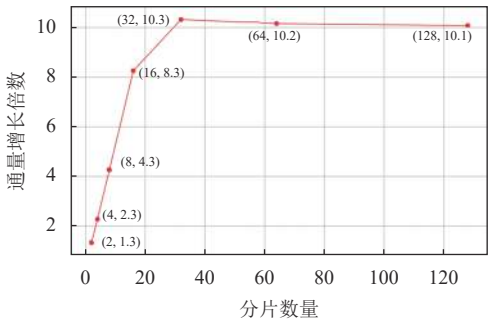


图 6 $\alpha=1, \beta=1, \Gamma=10^{-1}$ 时通量增长倍数与分片数量关系曲线

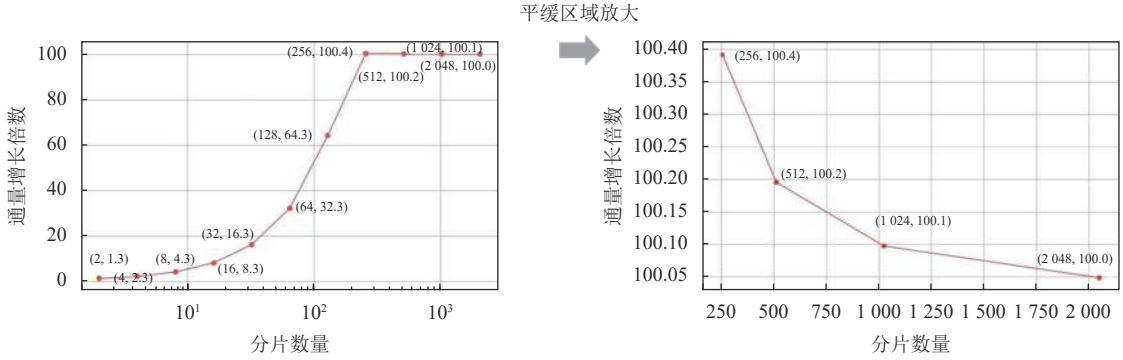


图 7 $\alpha=1, \beta=1, \Gamma=10^{-2}$ 时通量增长倍数与分片数量关系曲线

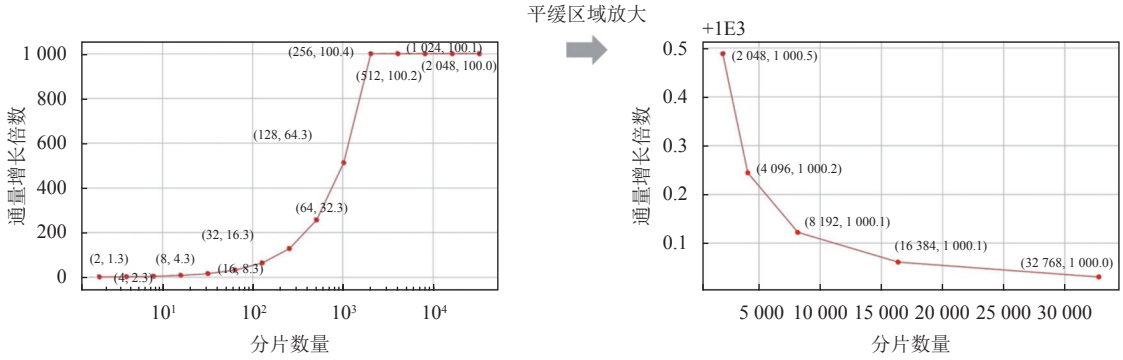


图 8 $\alpha=1, \beta=1, \Gamma=10^{-3}$ 时通量增长倍数与分片数量关系曲线

将不同主链复杂度情况下最高通量增长倍数时的分片数量汇总如表 2 所示, 通过不同数量级差下通量增长倍数与分片数量之间的关系曲线得到如下结论.

(1) 随着主链功能的复杂度变高, 中转所需要的时间更长, 则该通用星型分片架构下区块链的通量上限也会变得更低.

(2) 随着分片数量的增加, 尽管在某一最佳分片数量时通量达到了峰值, 但继续增加分片数量并不会大幅降低通量, 而是呈相对缓慢的下降趋势.

3.2.2 以片内交易为主的分片规则

目前已有一些研究工作致力于通过社群发现或机器学习的方式, 根据区块链网络中交易历史记录对账户进行分片, 使跨片交易所占比例降低, 并依然保证各分片交易划分相对均匀. 但在实际应用的区块链网络中, 按照地址均匀分片依然是最易于部署和实用性最强的. 在实际系统中引入调度算法需要周期性依照历史记录全局动态地调

整分片, 这对网络节点的计算和共识提出了更高的要求. 由于账户间的交易行为存在随机和不可预知的特征, 往往从全局视角经调度算法得到的分片策略依然存在相当比例的跨片交易, 其中一些经过充分优化后的分片策略理想情况下可以做到 70% 的交易是片内交易.

表 2　最高通量增长倍数时分片数量

$\alpha=1,\beta=1,\Gamma=10^{-1}$		$\alpha=1,\beta=1,\Gamma=10^{-2}$		$\alpha=1,\beta=1,\Gamma=10^{-3}$	
分片数量	通量增长倍数	分片数量	通量增长倍数	分片数量	通量增长倍数
2	1.3	2	1.3	2	1.3
4	2.3	4	2.3	4	2.3
8	4.3	8	4.3	8	4.3
16	8.3	16	8.3	16	8.3
32	**10.3**	32	16.3	32	16.3
64	10.2	64	32.3	64	32.3
128	10.08	128	64.3	128	64.3
256	10.04	**256**	**100.4**	256	128.3
512	10.02	512	100.2	512	256.3
1 024	10.01	1 024	100.1	1 024	512.3
2 048	10.005	2 048	100.05	**2 048**	**1 000.5**
4 096	10.002	4 096	100.02	4 096	1 000.2
8 192	10.001	8 192	100.01	8 192	1 000.1
16 384	10.000 6	16 384	100.006	16 384	1 000.06
32 768	10.000 3	32 768	100.003	32 768	1 000.03

另一种片内交易为主的分片情况是 Polkadot 网络中的中继链-平行链架构. Polkadot 的中继链负责网络的上层治理、平行链共识和跨片交易处理, 而每个平行链可以看作一个分片, 各自内部形成一个生态, 基础的业务仅在平行链内可以执行完成, 只有部分交易涉及和中继链的资产或其他平行链交互. 因此, 未来 Polkadot 中的片内交易很可能会占据较大的交易比例.

为探索经过调度算法或是在类似 Polkadot 网络中, 确保片内交易占据一定比例的分片策略的星型分片架构通量模型, 将片内交易比例 $g(N)$ 分别取 $\frac{1}{3}$, $\frac{1}{2}$, $\frac{2}{3}$ 列举在相对充分到很理想的调度类分片策略.

(1) 当片内交易比例取 $g(N)=\frac{1}{3}$ 时, 将公式 (19) 中 $f_{\max}(N)$ 和 $g(N)=\frac{1}{3}$ 代入公式 (15) 通用的通量性能模型中, 化简得:

$$(1+\sigma_{\max})\left(\frac{1+2\alpha+2\beta}{N}\right)=2\gamma \tag{24}$$

使主链达到性能瓶颈的临界分片数量 N':

$$N'=\frac{(1+2\alpha+2\beta)}{2\Gamma} \tag{25}$$

(2) 当片内交易比例取 $g(N)=\frac{1}{2}$ 时, 将公式 (19) 中 $f_{\max}(N)$ 和 $g(N)=\frac{1}{2}$ 代入公式 (15) 通用的通量性能模型中, 化简得:

$$(1+\sigma_{\max})\left(\frac{1+\alpha+\beta}{N}\right)=\gamma \tag{26}$$

使主链达到性能瓶颈的临界分片数量 N':

$$N'=\frac{(1+\alpha+\beta)}{\Gamma} \tag{27}$$

(3) 当片内交易比例取 $g(N)=\frac{2}{3}$ 时, 将公式 (19) 中 $f_{\max}(N)$ 和 $g(N)=\frac{2}{3}$ 代入公式 (15) 通用的通量性能模型中, 化简得:

$$(1+\sigma_{\max})\left(\frac{2+\alpha+\beta}{N}\right)=\gamma \tag{28}$$

使主链达到性能瓶颈的临界分片数量N':

$$N'=\frac{(2+\alpha+\beta)}{\Gamma} \tag{29}$$

公式 (25), 公式 (27), 公式 (29) 中得到的N'值便是分片数量N的临界值, 即通量达到最大的最佳分片数量, 由此可见在调度算法等使片内交易为主的分片规则中, 依然存在制约主链性能的分片数量上界.

结合公式 (7), 公式 (10) 依然可以推导出在使片内交易为主的分片规则下星型分片架构区块链的通量表达式为:

$$TPS=\begin{cases}\dfrac{1}{t}\cdot\dfrac{N^2}{(1+\sigma_{\max})[1+(\alpha+\beta)(N-1)]}, & N<N'\\ \dfrac{1}{t}\cdot\dfrac{N}{\gamma(N-1)}, & N\geqslant N'\end{cases} \tag{30}$$

观察公式 (30) 使片内交易为主的星型分片通量表达式和公式 (23) 普遍的均匀分片通量表达式可知, *TPS* 与分片数量N的关系依然是分段函数, 只是临界值发生了改变, 曲线趋势为: 开始时随着分片数量的增加, 通量随之线性增加. 当分片数量达到一个特定值时, 通量开始逐渐减少, 而非继续随之增加. 并且根据公式 (25), 公式 (27), 公式 (29) 可知, 随着片内交易比例$g(N)$的增加, 同等交易处理时间参数下, 使主链达到瓶颈的最佳分片数量N'也随之增加.

$$\frac{(1+2\alpha+2\beta)}{2\Gamma}<\frac{(1+\alpha+\beta)}{\Gamma}<\frac{(2+\alpha+\beta)}{\Gamma} \tag{31}$$

4 模型应用

4.1 以太坊 2.0

以太坊已明确表示将在以太坊 2.0 中以星型分片架构的方式将账户按照账户地址的前 6 位分到 64 个分片当中. 将抽象化的通用星型分片架构与普遍采用的均匀分片下的通量模型在以太坊项目上应用. 在给定分片数量的情况下, 可以通过公式 (20) 直接计算交易处理时间参数 α,β,γ 或 Γ 的最佳比例. 令分片数量$N=64$为最佳分片数量, 反推在最佳分片数量时, 各类型交易处理时间参数的数量关系.

$$N=\frac{(\alpha+\beta+\Gamma)+\sqrt{(\alpha+\beta+\Gamma)^2-4\Gamma(\alpha+\beta-1)}}{2\Gamma} \tag{32}$$

依然假设片内交易、发送跨片交易、接收跨片交易这 3 种的处理时间处于同一数量级. 将$\alpha=1$, $\beta=1$, $N=64$代入公式 (32), 得到:

$$\Gamma=\frac{127}{4032}\approx 0.0315 \tag{33}$$

因此, 对于以太坊 2.0 来说, 将主链交易处理时间参数Γ控制在 0.031 5 附近, 即取交易归属概率分布波动上界$\sigma_{\max}=1$, 参数γ控制在 0.015 7 附近, 则 64 便恰好为最优分片数量.

$$\gamma=\frac{\Gamma}{(1+\sigma_{\max})}\approx 0.0157 \tag{34}$$

若γ的值更大, 意味着主链更慢, 则最优分片数量会小于 64, 但性能影响较小; 若γ的值更小, 意味着主链更快, 则最优分片数量会大于 64, 性能影响较大, 说明 64 个分片并未充分发挥分片的性能, 再增加分片数量会使通量得到明显的提升.

4.2 Polkadot

Polkadot 项目未来上线平行链功能后, 会对平行链插槽进行逐个拍卖, 其最终愿景是能够支撑 100 个平行链接入中继链. 在 Polkadot 的中继链-平行链架构中, 中继链可视为主链, 平行链可视为分片链, 符合星型架构中跨片

交易通过主链转发的特点, 但其各分片自成一个生态, 相比于少数需要跨链的业务, 片内的业务流转更加频繁. 其片内交易天然占据交易的大部分比例, 适用于片内交易为主的星型分片架构通量模型.

在已知目标分片数量$N=100$, 但未知片内交易比例$g(N)$和主链功能复杂度对交易处理时间参数的影响情况下, 可以将公式 (19) 中$f_{\max}(N)$和分片数量$N=100$代入公式 (15), 化简得:

$$\frac{\dfrac{g(N)}{1-g(N)}+\alpha+\beta}{\Gamma}=100,\ 0<g(N)<1;\ \alpha\approx\beta\approx 1 \tag{35}$$

其中, $\dfrac{g(N)}{1-g(N)}$是片内交易比例$g(N)$的单调递增函数, 可获得在保持最佳分片数量不变的情况下, 片内交易比例和交易处理时间参数间的关系. 随着片内交易比例的增加, Γ也随之增加, 即对中继链处理交易速度要求降低, 功能可以更加复杂.

Polkadot 平行链功能上线后, 片内交易按照设计较大概率占据多数, 假设在系统中片内交易比例占 90%, 将$g(N)=0.9$, $\alpha=1$, $\beta=1$ 代入公式 (35), 得到:

$$\Gamma=0.11 \tag{36}$$

那么将中继链交易处理时间参数Γ控制在 0.11 附近, 便可支撑接入 100 个平行链, 且刚刚触及性能瓶颈. 另外, 由于 Polkadot 中平行链是逐个上线, 而非一次性分配完毕, 未来可以通过本模型在平行链功能上线早期, 根据初始几个平行链与中继链运行的网络参数来推算出使通量达到最大的平行链数量, 对后续中继链网络优化和拟定分片数量做进一步指导.

5 结 论

1) 本文首次将国际上主流的区块链并行化方案及应用按照组织架构分成星型架构和平行架构两类, 针对不同的星型分片架构方案抽象出了一种通用的区块链星型分片架构, 并对该通用架构中的交易过程进行了量化建模.

2) 量化得到理论上区块链通量与分片数量的关系, 从而得到在普遍分片规则下的星型分片架构通量模型. 该模型证明了, 随着分片数量N的增加, 区块链通量先是随之增加, 当分片数量N达到一个特定值后, 使分片中的交易处理时间与主链的交易处理时间相等, 即$t_i=t_{\text{mainchain}}$, 主链的处理速度刚刚达到瓶颈, 此后再增加分片数量N会使通量不增反减. 因此, 此时区块链系统的通量达到最大, 当前的分片数量N便是最佳的分片数量. 分别分析目前普遍采用的均匀分片规则和片内交易为主的分片规则两类情况, 求得使得区块链的通量达到最大的最佳的分片数量N'. 在该临界值之前, 通量呈线性稳定增加; 在临界值后, 通量会缓慢地下降, 且有下界.

3) 以主流的星型分片架构方案以太坊 2.0 和 Polkadot 为例, 应用性能模型于现有并行化场景. 分别按照以太坊 2.0 的地址分片规则 (按照地址将账户分为 64 个分片) 和 Polkadot 中继链+100 条平行链架构中片内交易为主的分片规则, 分析最优的片内交易与跨片交易的速度关系. 该模型可以为采用星型分片架构的区块链项目提供分片数量与主链功能复杂度的参考, 以期系统通量达到理论上限.

References:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[2] Wood G. Ethereum: A secure decentralised generalised transaction ledger Berlin version. 2020. https://ethereum.github.io/yellowpaper/paper.pdf

[3] Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y, Muralidharan S, Murthy C, Nguyen B, Sethi M, Singh G, Smith K, Sorniotti A, Stathakopoulou C, Vukolić M, Cocco SW, Yellick J. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proc. of the 13th EuroSys Conf. Porto: ACM, 2018. 30. [doi: 10.1145/3190508.3190538]

[4] Cachin C. Architecture of the hyperledger blockchain fabric. In: Proc. of the 2016 Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Chicago, 2016. 1–4.

[5] Burdges J, Cevallos A, Czaban P. Overview of Polkadot and its design considerations. 2020. https://github.com/w3f/research/blob/master/docs/papers/OverviewPaper-V1.pdf

[6] EthHub. Ethereum 2.0 phases. 2020. https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/

[7] The ZILLIQA Team. The ZILLIQA technical whitepaper. 2019. https://docs.zilliqa.com/whitepaper.pdf

[8] Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Syta E, Ford B. OmniLedger: A secure, scale-out, decentralized ledger via sharding. In: Proc. of the 2018 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2018. 583–598. [doi: 10.1109/SP.2018.000-5]

[9] Zamani M, Movahedi M, Raykova M. RapidChain: Scaling blockchain via full sharding. In: Proc. of the 2018 ACM SIGSAC Conf. on Computer and Communications Security. Toronto: ACM, 2018. 931–948. [doi: 10.1145/3243734.3243853]

[10] Wang JP, Wang H. Monoxide: Scale out blockchain with asynchronous consensus zones. In: Proc. of the 16th USENIX Conf. on Networked Systems Design and Implementation. Boston: USENIX Association, 2019. 95–112.

[11] Al-Bassam M, Sonnino A, Bano S, Hrycyszyn D, Danezis G. Chainspace: A sharded smart contracts platform. In: Proc. of the 25th Annual Network and Distributed System Security Symp. San Diego: The Internet Society, 2018. 1–15.

[12] MultiVAC Foundation. MultiVAC: A high-throughput flexible public blockchain based on trusted sharding computation. 2018. https://www.mtv.ac/assets/file/MultiVAC_Tech_Whitepaper.pdf

[13] Swan M. Blockchain: Blueprint for A New Economy. Sebastopol: O'Reilly Media, 2015.

[14] Buterin V. Why sharding is great: Demystifying the technical properties. 2021. https://vitalik.ca/general/2021/04/07/sharding.html

[15] Proof-of-stake (POS). 2021. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[16] Delegated proof of stake (DPoS). 2020. https://www.geeksforgeeks.org/delegated-proof-of-stake/

[17] Garzik J. Block size increase to 2MB. 2019. https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki

[18] Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Sirer EG, Song D, Wattenhofer R. On scaling decentralized blockchains. In: Proc. of the 2016 FC Int'l Workshops on Financial Cryptography and Data Security. Christ Church: Springer, 2016. 106–125. [doi: 10.1007/978-3-662-53357-4_8]

[19] Lombrozo E, Lau J, Wuille P. Segregated witness (cosensus layer). 2021. https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[20] Li CX, Li PL, Zhou D, Yang Z, Wu M, Yang G, Xu W, Long F, Yao ACC. A decentralized blockchain with high throughput and fast confirmation. In: Proc. of the 2020 USENIX Annual Technical Conf. USENIX Association, 2020. 515–528.

[21] Yu GS, Wang X, Yu K, Ni W, Zhang JA, Liu RP. Survey: Sharding in blockchains. IEEE Access, 2020, 8: 14155–14181. [doi: 10.1109/ACCESS.2020.2965147]

[22] Poon J, Dryja T. The Bitcoin lightning network: Scalable off-chain instant payments. 2016. https://lightning.network/lightning-network-paper.pdf

[23] Raiden Network. What is the raiden network? 2020. https://raiden.network/101.html

[24] Singh A, Click K, Parizi RM, Zhang Q, Dehghantanha A, Choo KKR. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. Journal of Network and Computer Applications, 2020, 149: 102471. [doi: 10.1016/j.jnca.2019.102471]

[25] Bagui S, Nguyen LT. Database sharding: To provide fault tolerance and scalability of big data on the cloud. International Journal of Cloud Applications and Computing, 2015, 5(2): 36–52. [doi: 10.4018/IJCAC.2015040103]

[26] Costa CH, Vianney J, Maia P, et al. Sharding by hash partitioning—A database scalability pattern to achieve evenly sharded database clusters. In: Proc. of the 17th Int'l Conf. on Enterprise Information Systems. Barcelona, 2015. 313–320. [doi: 10.5220/0005376203130320]

[27] Luu L, Narayanan V, Zhang CD, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 17–30. [doi: 10.1145/2976749.2978389]

[28] Li WL. Ethereum throughput bottleneck analysis and optimization research [MS. Thesis]. Xiangtan: Xiangtan University, 2020 (in Chinese with English abstract). [doi: 10.27426/d.cnki.gxtdu.2020.001328]

附中文参考文献:

[28] 李雯林. 以太坊吞吐量瓶颈分析与优化研究 [硕士学位论文]. 湘潭: 湘潭大学, 2020. [doi: 10.27426/d.cnki.gxtdu.2020.001328]

王柯元(1997－), 男, 博士生, CCF 学生会员, 主要研究领域为区块链, 数字货币.

姜鑫(1996－), 男, 硕士生, 主要研究领域为区块链, 数字货币.

贾林鹏(1995－), 男, 博士生, CCF 学生会员, 主要研究领域为区块链, 数字货币.

段田田(1996－), 女, 博士生, CCF 学生会员, 主要研究领域为区块链, 数字货币.

孙毅(1979－), 男, 博士, 博士生导师, CCF 杰出会员, 主要研究领域为区块链, 数字货币.