基于分片技术的区块链可扩展性研究综述

蒋凌云,杨京霖,马鹏程,叶 飞,徐 佳,刘婷婷*
(南京邮电大学计算机学院、软件学院、网络空间安全学院,江苏南京 210003)

摘 要: 区块链存在资源消耗大、吞吐量低等问题,严重影响区块链技术的落地应用. 分片技术为解决区块链可扩展性问题提供了可行的方案. 本文首先结合区块链逻辑结构对不同层级的区块链可扩展性方案进行总结. 然后从分片结构层次、系统运行流程、研究问题、功能组件4个不同的角度对分片区块链进行概述. 本文将分片区块链的设计分为9个功能组件,在此基础上,从功能组件视角总结了分片区块链的研究现状,详细地介绍了典型的分片方案. 最后,从安全、性能以及均衡性角度讨论了分片技术当前所面临的挑战,并对未来研究进行了展望.

关键词: 分片方案;区块链;功能组件;可扩展性;逻辑层级
基金项目: 国家自然科学基金(No.62372250,No.62171217);南京邮电大学引进人才科研启动基金(自然科学)(No.NY223169)
中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112(2025)07-2579-22
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20241117

Research on Scalability of Blockchain Based on Sharding: A Survey

JIANG Ling-yun, YANG Jing-lin, MA Peng-cheng, YE Fei, XU Jia, LIU Ting-ting*
(*School of Computer Science*, *Nanjing University of Posts and Telecommunications*, *Nanjing*, *Jiangsu* 210003, *China*)

Abstract: The blockchain has some scalability issues such as high-resource consumption and low-level throughput, which seriously affects the application of blockchain technology. Sharding technology provides a feasible solution to the scalability issues of blockchain. In this paper, the various scalability solutions based on logic architecture of blockchain are introduced firstly, then, the sharding technology is summarized from four aspects: sharding hierarchy, system operation, key problems, and functional components. The design of sharding blockchain is decomposed into nine functional components, on this basis, the existing works of sharding blockchain are analyzed from the perspective of functional components, and the details of these typical sharding solutions are presented. Finally, the current research challenges faced by sharding technology are discussed from the perspectives of security, performance, and balance. Also, the future research directions of development process and simulation are provided.

Key words: sharding scheme; blockchain; functional component; scalability; logic architecture
Foundation Item(s): National Natural Science Foundation of China (No.62372250, No.62171217); Natural Science Research Start-Up Foundation of Recruiting Talents of Nanjing University of Posts and Telecommunications (No.NY223169)

1 引言

区块链技术起源于比特币系统[1],使用分布式信任模型取代中介代理模型[2],具有透明性、去中心化、防篡改等重要特征,被广泛应用于金融、政务、民生等诸多领域[2~5]. 区块链的可扩展性(Scalability)指的是区块链系统在交易量增加时仍能保持高效运行的能力. 主流的传统区块链(如比特币和以太坊)因采用全网共识和单链结构,导致交易处理能力受到严重限制. 例如,比特币网络的系统每秒处理的交易数量(Transactions Per Second,TPS)仅约7笔,这远远无法满足大规模应用的需求. 相比之下,Visa官方公布的峰值处理能力为6.5万TPS,区块链在可扩展性上的短板显而易见. 研究表明区块链存在安全性、可扩展性和去中心化的三者制衡[6~11],即在保障去中心化和安全性的同时,提升可扩展性往往面临挑战. 因此,如何突破区块链的吞吐量瓶颈,提升可扩展性,已成为当前区块链技术发展需要解

收稿日期:2024-12-12;录用日期:2025-05-06;责任编辑:覃怀银
*通讯作者:刘婷婷

决的核心问题之一.

区块链可扩展性问题可分为功能扩展和性能扩展,功能扩展指增加区块链系统的功能模块、协议或技术,以适应更多的应用,如支持分布式应用、提供跨链数据交互等;性能扩展指采用不同的技术和方法,提升系统的处理速度,增大区块链吞吐量,降低确认时延,或是提升系统安全性,以满足不断增长的用户规模和交易需求,现有的性能扩展方案可分为链下扩展(如支付通道、侧链等)与链上扩展[如分片、有向无环图(Directed Acyclic Graph,DAG)等]两类.

支付通道技术利用链下微支付来减少主链负载,交易不需全网共识,仅在通道打开和关闭时需要主链确认,但需预先抵押资金到通道,流动性受限. 侧链技术通过将交易分流至独立子链减少主链负载,不同子链可以采用不同的共识机制,但依赖跨链桥机制进行交易迁移,导致跨链桥容易成为安全攻击高发目标,同时许多侧链依赖少数验证者的情况也会导致中心化并带来安全隐患. 有向无环图(DAG)采用并行交易确认机制突破单链结构限制,但容易面临双花攻击和分叉,存在较大安全性问题. 分片技术通过分片架构(网络分片、交易分片、状态分片)实现系统性扩展,将全网节点划分为若干并行链,理论上实现线性扩展的同时维持了安全性与去中心化平衡,为提升区块链可扩展性提供了解决方案,引发了大量研究者的关注. 然而,尽管分片技术具备显著优势,如何高效、安全地处理不同分片之间的跨片交易和信息同步以及如何根据网络负载情况动态调整分片的数量和大小来平衡性能和安全性仍然是需要突破的核心挑战.

在过去的几年中,研究人员提出了不同的分片技术来解决这些问题. 然而,目前还缺少文献总结和展示区块链分片技术领域的进展. 本文旨在对区块链分片技术的研究进展进行系统性梳理,并结合UTXO(Unspent Transaction Output)与Account/Balance模型对典型方案进行横向对比,展望未来研究的方向与相关挑战.

本文的主要贡献如下:对分片区块链方案进行总结的基础上抽象出九个功能组件,有利于完善区块链分片技术协议;提出了基于代理人机制的账本数据迁移方案,提高账本迁移效率;提出了基于信誉值的MPT(Merkle Patricia Trie)树结构记录账户节点信誉,为安全性提供保障;提出了分片列式学习存储架构提高存储效率.

2 背景知识

2.1 区块链可扩展性问题的评价指标

在文献[12]中,Croman等人针对比特币系统可扩展性评价,提出了以吞吐量(throughout)、时延(latency)、初始化引导时间(bootstrap time)、确认每笔交易的开销(cost per confirmed transaction)作为几个关键评价指标. 其中,吞吐量和时延是最主要的两个指标,也是与用户体验(quality of experience)直接相关的性能指标. 吞吐量指系统每秒处理的交易数量,单位为Transatction/s(简记为TX/s,也可简记为TPS). 时延指从交易发起到交易被最终确认之间的整体交易时延,由网络时延和共识时延组成. 网络时延指从发起交易请求到被全网确认接收之间的时间延迟,是由分布式网络结构、路由协议和网络通信状态等因素决定的. 共识时延是指执行共识算法所带来的时延.

除了相关的性能评价指标之外,还需要考虑系统安全性评价指标. 系统弹性(system resiliency)指系统中可以容忍的最大恶意节点比例,是区块链安全性能的主要评价指标. 在基于分片的区块链系统中,不仅需要考虑系统弹性,还需要考虑分片弹性(shard resiliency). 分片弹性指在保证分片安全的前提下,分片内部可以容忍的最大恶意节点比例. 分片技术会稀释系统算力,导致分片弹性小于系统弹性.

2.2 区块链可扩展性方案分析

区块链可扩展性研究可以分为第0层、第1层和第2层扩展方案[8~11]. 第0层扩展方案通过优化底层的数据传输协议减少传播延迟来提升性能;第1层扩展方案也称为链上扩展方案,通过对区块链自身的协议和体系结构进行改进来提升扩展性;第2层扩展方案也称为链下扩展方案,通过链外的方法扩展提升区块链系统的性能与扩展性. 在文献[10]的多层方案基础上,本文依据区块链的逻辑结构对相关的可扩展性方案进行分析总结,如图1所示.

(1)第0层. 物理层通过改进底层网络传输协议和构建更强健的点对点(Peer-to-Peer,P2P)网络实现扩展,可以设计实现了高效的分发网络和路由算法,帮助区块或交易快速传播[13,14],也可以设计新的拓扑结构,提高了网络的块传播速度[15].

(2)第1层. 第1层逻辑结构包括数据层、网络层、共识层和激励层. 数据层负责区块和系统账本的组织和存储,因此数据层的扩展方案主要针对区块、账本和存储等方面进行扩展. 在区块方面,可以通过压缩区块来减少传播的信息量[16];在账本方面,可以利用DAG的并行性质改变传统的单链结构,提高系统处理效率[17~20];在存储方面,可以考虑协作式存储方案[21,22]和轻节点存储方案[1]. 网络层主要有分片(sharding)[22~56]和轻节点支付验证(Simplified Payment Verification,SPV)[1]两种方案.

共识层主要负责共识协议的设计,根据一致性原

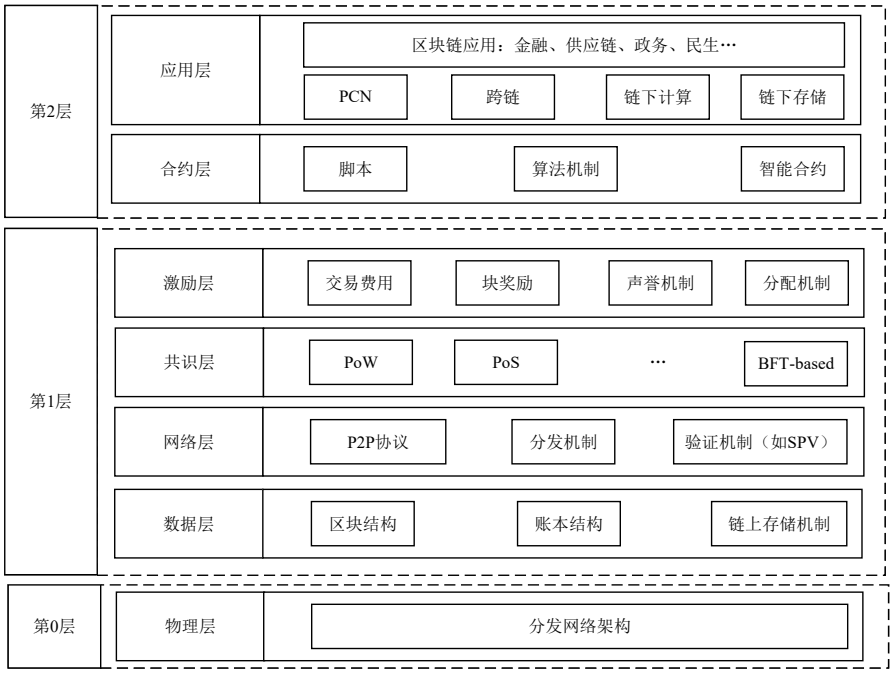


图1　区块链逻辑结构及扩展思路概要

则可以将共识协议分为强一致性共识协议和弱一致性共识协议两类. 在强一致性共识协议中,当区块通过验证时,即可认为交易被最终确认,共识结果唯一,不存在分叉的可能. 强一致性共识协议的典型方案有证明类共识协议和基于拜占庭容忍机制(Byzantine Fault Tolerance,BFT)类的共识协议,证明类的典型共识协议有委托权益证明(Delegated Proof of Stake,DPoS)[57~59]等,BFT类的典型共识协议有对BFT的改进FABC(Fast Authenticated Byzantine Consensus)协议[60],使用PBFT[61](Practical Byzantine Fault Tolerance)进行扩展的Hyperledger Fabric[62]等;在弱一致性共识协议中,单个节点作为合法区块生成者(非唯一),交易被打包进区块后需要后续若干区块的确认,交易才能被最终确认,其共识结果在一定的时间内被颠覆可能性较大. 弱一致性共识协议的典型方案是工作量证明(Proof of Work,PoW)共识协议[62~65]和权益证明(Proof of Stake,PoS)协议[66~68]. 共识协议是区块链系统的基石,是影响区块链扩展的主要因素,同时也是研究中的难点,更多的区块链共识方面的工作可以参阅文献[69].

激励层方案主要从改进区块链固有的奖励模型和提出新的激励两个方面进行研究. 区块链的固有奖励主要包括交易费用和出块奖励两个部分. 出块奖励一般设为协议规定的常数,因此解决方案多集中在交易费用方面,例如,可以通过势博弈对交易费用定价减少跨分片交易和最大化系统吞吐量[70],可以通过"分片奖励(shard reward)"来鼓励小分片合并,避免节点闲置,减少空区块的产生[36],也可以将声誉和激励挂钩,规范节点行为[27].

(3)第2层. 第2层逻辑结构包括合约层和应用层. 合约层解决方案提供智能合约[71,72]以及智能合约的支撑[73]. 应用层方案基于底层区块链实现实际应用,通过链外技术实现功能性的扩展. 典型的链外技术有支付通道网络(Payment Channel Network,PCN)[74~80]方案、跨链技术(cross-chain)[81~85]、链下计算(off-chain computation)技术[86,87]、链外存储方案[88~91].

分片技术通过将串行的单链结构调整为并发的多链结构,将传统单链的计算、存储和共识负载分散到多个子链(分片)中,从而实现性能的线性扩展,为解决区块链可扩展性问题提供了可行的解决方案.

3　分片区块链概述

3.1　分片区块链的结构层次

从分片结构层次视角,分片技术可分为网络分片、交易分片和状态分片. 网络分片作为分片技术的基础,将网络中的验证者节点分组,减小单个P2P网络的规模,降低通信开销,并为系统提供并发基础. 交易分片将交易全集进行划分和分配,使得不同分片处理相互独立的交易子集. 状态分片分割完整账本,令不同分片中节点仅维护自身分片的账本,并保证各分片账本之间不存在冲突的情况下能组合成一个唯一的完整账本.

系统运行时网络中的交易组成“交易池”[也称为内存池(memory pool)],这些交易由账户向网络提交产生. 对于交易来说,可将交易分为普通交易(单个分片可验证)和跨分片交易(多个分片协作验证). 为了方便后续说明,图2假设基于账户的公钥(Public Key,PK)可分为两组账户,可以通过对其账户公钥地址的首位进行模2运算确定其所属分片. 账户向网络提交的交易被汇总到交易池中. 交易分片算法将交易池中的交易划分成若干相互独立的交易子集. 例如,在图2中,交易池中交易根据发起者的不同被划分成交易分片1和交易分片2. 网络分片算法将网络中的节点划分成若干个节点子集,对应于图2中的网络分片1和网络分片2.

运行时,每个网络分片运行共识算法独立完成交易分片子集的验证工作,并产生各自的分片账本,如图2中网络分片2独立完成普通交易的验证,内部共识形成区块并记录到分片2账本. 但对于特殊的跨分片交易,需要多个网络分片协作完成. 如图2所示,对于交易分片1中的跨分片交易,网络分片1需要和网络分片2协作验证,验证结果经过共识被打包进区块,并附加到分片1账本和分片2账本.

状态分片指将区块链系统的状态进行划分,其中状态是指系统在某个时刻的数据视图,如以太坊中的状态可以简单理解为某个时刻下系统所有账户的余额视图. 在图2中,分片1账本存储账户组1的状态和交易历史,分片2账本存储账户组2的状态和交易历史. 状态分片技术保障分片1账本和分片2账本的合法性和正确性,可以减少节点的存储负担和数据冗余.

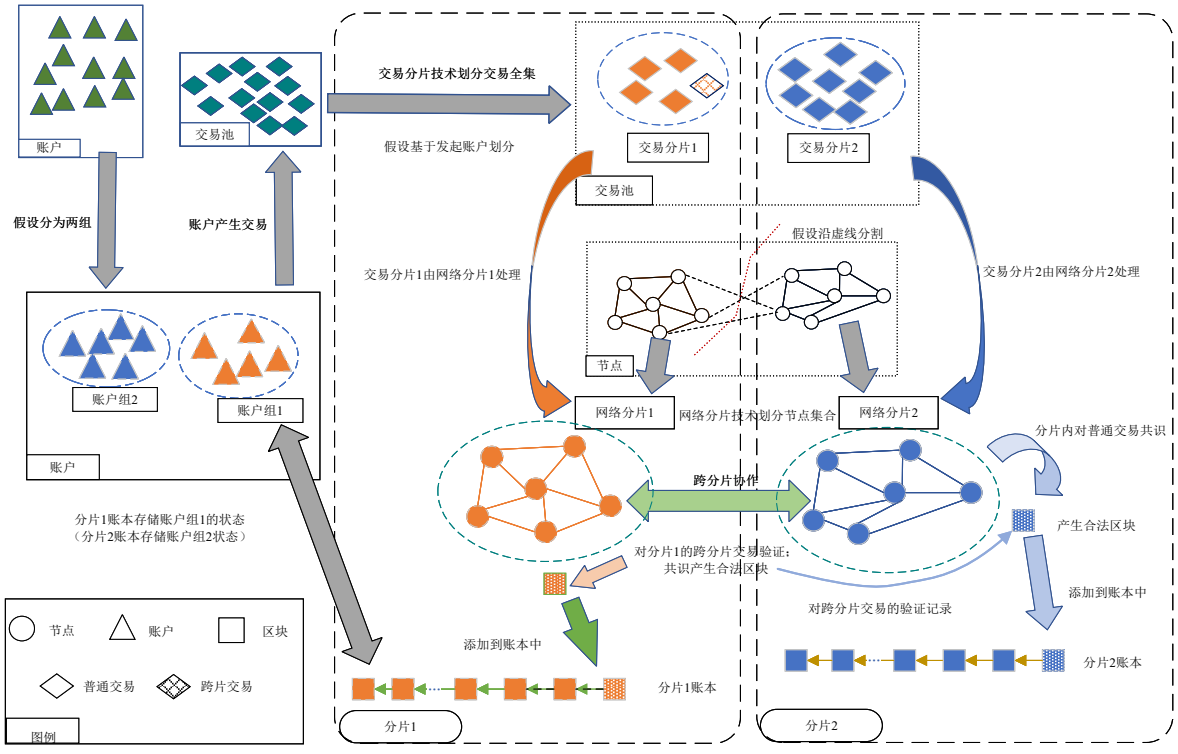


图2 基于账户的分片系统结构层次示意图

3.2 分片区块链系统的运行

从系统运行视角看,分片方案由分片建立、系统运行和分片重组3个阶段构成. 分片建立阶段是整个运行纪元的预备阶段,完成对节点的分配和P2P网络的构建,以及相关初始引导工作. 系统运行阶段主要完成交易的验证和共识,对外提供服务. 分片重组阶段对分片区块链系统进行重新配置,确定新的分片结构,增强系统的随机性和动态性. 分片方案设计时需要考虑的问题主要包括网络分片策略、交易分片策略、片内共识策略、跨分片策略和分片重组策略. 一般来说,分片建立阶段仅在系统初始化时期进行一次,此后分片由系统运行阶段和分片重组阶段交替,形成一个个分片纪元. 但考虑到更加动态的情况,如纪元交替期间,分片系统调整节点分配规则、交易分配规则,那么分片系统的纪元之间就不是简单的阶段重复. 因此,本文将分片纪元分为3个阶段.

3.2.1 分片建立阶段

分片建立阶段是预备阶段,首先基于有利于系统发展的原则,在参与本轮分片纪元的节点中选择若干节点,按照网络分片算法将被选中的节点划分成若干

分组,形成若干个网络分片. 分片建立阶段主要分为身份注册、分片配置、委员会建立3个部分.

身份注册旨在验证加入节点的合法性以限制恶意节点. 在这一过程中,节点需要向系统注册其身份信息,包括公钥、互联网协议(Internet Protocol,IP)地址等. 在非许可区块链中,节点身份注册是公开的,因此区块链中的节点的信任度较低. 为了防止Sybil攻击(即恶意节点通过伪造多个身份加入网络),注册过程往往要求节点提供一定的质押(如一定数量的加密货币)或者解决PoW难题(如RapidChain[25]、RepChain[27]等)来验证身份. 在许可区块链中,由于参与者具备一定的可信度或身份已得到确认,节点身份注册是一个受控过程. 因此无须代价高昂的挖矿难题来验证身份,往往通过传统的身份验证或基于数字证书的加密身份认证来实现(如Hyperledger Fabric[62]等).

在每个纪元开始时,区块链系统通常使用随机函数决定节点在整个纪元内的分配方式,目的是提高系统随机性,确保系统的安全性和公平性. 由于非许可区块链公开透明的特性,恶意节点通过预测节点分配结果对系统发动攻击的可能性更大,因此在非许可区块链中纪元随机性往往更加重要[如Elastico[23]采用epochRandomness函数、OmniLedge[24]采用RandHound+VRF(Verifiable Random Function)-based等]. 在许可区块链中,由于参与者已经过验证,可以采用更简单、更传统的随机数生成机制(如AHL[34]采用无偏随机数rnd生成分片方案). 引入随机性可以有效防止恶意节点预测或操纵节点的分配,提升系统的抗攻击能力. 此外,随机性还可以避免某些分片负载过重或过轻的情况,进一步提升系统的平衡性和可靠性.

绝大多数分片方案在分片建立阶段还需要建立委员会. 委员会涉及管理分片的状态、共识机制、跨分片通信以及对整个网络的动态调整等方面的任务. 在非许可区块链中,通常根据随机数生成机制将所有注册节点划分为若干个委员会,每个委员会负责一个或多个分片的共识工作. 例如,RapidChain[25]通过从低一层的节点持续随机组合选取出root group,接着由root group担任委员会并完成接下来的分片配置. 在许可区块链中,委员会组建可以更加集中化和高效. 例如,SharPer[41]通过考虑节点的地理位置来建立委员会(或称为集群),将地理位置接近的节点分配到同一委员会中,显著减少彼此通信的延迟,从而提高系统的响应速度和效率.

3.2.2　系统运行阶段

系统运行阶段主要对交易进行处理,除此以外,开放性网络允许节点在运行阶段自由地加入和离开,使得网络呈现强动态性,运行阶段还需要对此进行处理. 如SSChain[30]针对动态性网络,设计了市场激励机制维护系统安全.

系统运行阶段对处理交易可分为提交、路由、共识3个阶段. 本节结合基于UTXO模型的分片方案RapidChain[25]和基于Account模型的分片方案BrokerChain[28]的交易处理流程进行阐述.

(1)基于UTXO模型的分片方案交易流程

(a)提交阶段:用户通过客户端或代理把交易提交给任一节点. 在提交阶段,可以通过客户端优化算法对交易进行预处理. 如图3所示,在步骤a中,交易TX被提交到分片2,由共识委员会C_2进行处理,随即进入路由阶段.

(b)路由阶段:接收交易的节点根据交易的地址和分片建立阶段所确定的交易分配规则,将交易路由到处理交易的目标分片. 在路由阶段,节点查找自己的路由表确定下一跳,一般需要经过多跳才能到达目标分片. 如图3步骤b所示,交易TX的输入来自分片1和分片2,输出为分片3,因此首先将交易TX路由至目标分片3. 共识委员会C_3对交易TX进行拆分,创建两个子交易TX_1和TX_2,以及最终交易TX_3. 然后发起路由步骤c,将TX_1和TX_2分别路由至目标分片1和目标分片2.

(c)共识阶段:当交易通过所建立的路由进入目标网络分片后,交易会在目标网络分片中的节点之间进行传播(如果存在共识委员会或共识领导者,他们将负责收集交易并承担内部广播责任). 接着,根据确定的共识协议对交易进行验证,当共识通过,交易被记录到分片账本. 对于跨片交易,共识阶段还包括多个分片之间的协同阶段,目标分片需要反馈交易的验证结果,如图3中步骤d所示,分片1和分片2在步骤d.1和步骤d.2中返回对TX_1和TX_2的验证结果,分片3根据返回的结果对TX_3进行验证,从而完成对跨片交易TX的验证.

(2)基于Account模型的分片方案交易流程

(a)提交阶段:在Account模型中,发起的原始交易涉及发送方账户和接收方账户,这些账户可能分布在不同的分片中,往往通过中介账户或者委员会等进行交易拆分转移. 如图4所示,账户A发起原始交易TX(包括代币锁定持续时间H_{lock}),并将该交易发送给中介C_1.

(b)路由阶段:交易被拆分为对应的中继交易之后由相关机构转发到相关的分片. 如图4所示,中介C_1首先创建TX_1并将TX_1发送到源分片即分片1,源分片节点验证TX_1. 中介账户C_1确认TX_1已被源分片确认之后立即创建TX_2,并路由至目标分片即分片2.

(c)共识阶段:交易进入目标分片,分片节点根据账户状态进行验证. 若交易涉及多个分片,目标分片间需协同验证. 如图4所示,分片2节点获得记账权后对TX_2进行验证,将验证通过的交易存储在本地交易池中

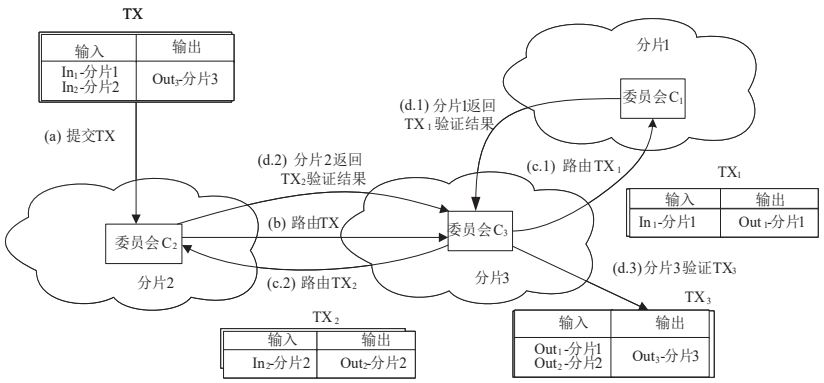


图3 基于RapidChain的系统交易处理流程

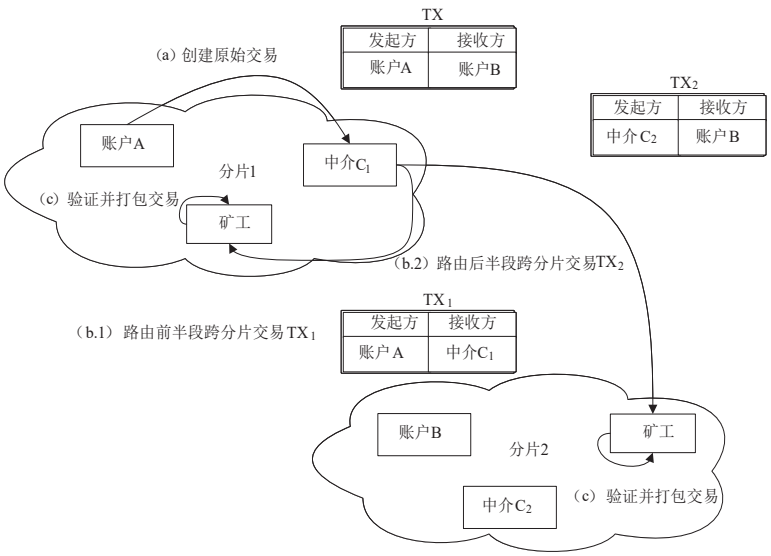


图4 基于BrokerChain的系统交易处理流程

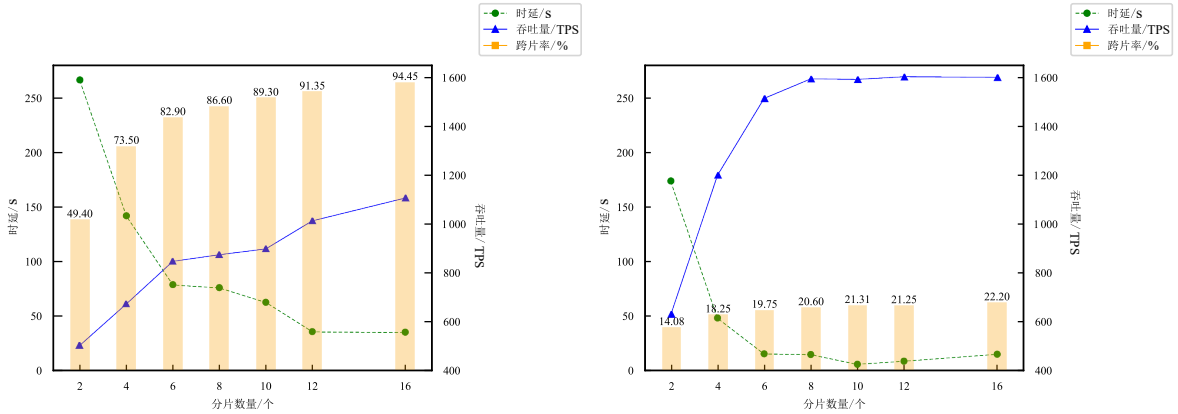
等待打包,如果此时分片1的当前区块高度小于$H_{current}+H_{lock}/2$,则将TX_2打包进新区块,并更新账户状态. 通过跨分片的通信协调,从而实现整个交易的原子性,确保数据一致性.

图5展示了Monoxide和BrokerChain在不同分片数量下的吞吐量、跨片交易比例以及交易时延. 从图5(a)可以看出Monoxide方案在分片数量低于16时,随着分片数量的增加,交易确认时延显著降低,吞吐量同步提升,但跨分片交易比例也会增长,当分片数量达到16时,跨分片交易的比例已经接近于100%,频繁的跨片交易成为了限制区块链性能扩展的瓶颈. 不同于Monoxide,BrokerChain在重配置阶段通过账户划分降低跨片交易比例,从图5(b)可以看出该方案在提高吞吐量的同时有效降低了跨片交易比例与时延. 由此看出分片重配置是降低跨分片交易比例和解决性能扩展瓶颈的有效方法之一.

3.2.3 分片重配置阶段

随着系统的不断运行,网络中的节点会随着时间不断增加,可能出现多种问题,例如,分片间负载不均衡导致中心化、恶意节点发动腐败攻击(corruption attack)提升恶意节点比例或学习分片规则从而针对性地创造身份导致恶意节点聚集等.

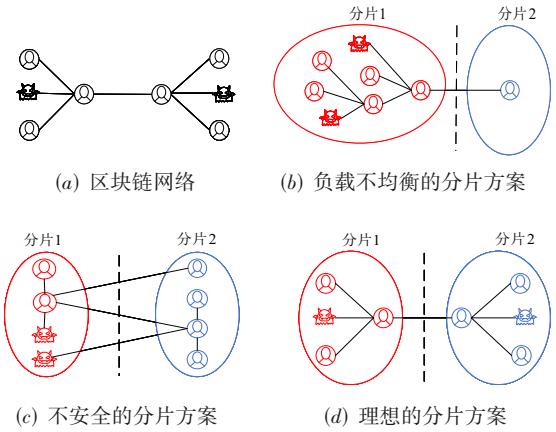
例如,图6(a)展示了由8个节点和7条边组成的区块链网络,其中有2个潜在的恶意节点,边表示节点之间存在交易. 在图6(b)中可以看出,在这种分片方案下有1笔跨分片交易,但是分片1需要处理7笔交易,而分片2只需要处理1笔交易,2个分片之间负载不均衡指数达到了6. 在图6(c)中,2个分片之间的负载是完全均衡的,但是这种分片方案却产生了3笔跨分片交易,同时由于账户划分不当也给分片1带来了潜在的安全问题. 理想的分片方案如图6(d)所示,在保证每个分片系统安全的前提下,实现最少的跨分片交易和最均衡的工作负载. 从上面的例子不难看出,一个好的账户分片方案,不仅能降低跨分片交易数量,保证每个分片的负载均衡,还能使恶意账户均匀分布在不同分片内. 但在最初的分片建立阶段,并不能确定节点是否为恶意



(a) Monoxide不同分片规模的性能比较　　(b) BrokerChain不同分片规模的性能比较

图5　不同分片规模下区块链系统的时延、TPS以及跨片交易率

节点,因此需要在分片重组阶段设计合理的重组方案,在保证系统安全的同时,降低跨片交易数量和负载均衡.



(a) 区块链网络　(b) 负载不均衡的分片方案

(c) 不安全的分片方案　(d) 理想的分片方案

图6　不同分片方案的对比

分片重配置在基于UTXO模型和基于Account模型的分片方案中同样存在差异.

(1)基于UTXO模型的分片重配置. 在基于UTXO模型的分片系统中,分片重配置主要关注节点的重新分配,以降低负载不均衡和腐败攻击的风险. 通过使用随机数生成机制重新分配部分节点到不同分片,确保节点分布的均衡性和随机性,防止恶意节点集中在某一分片. 例如,Elastico[23]在每个分片纪元结束后使用Randomness函数对整个网络的节点进行重新配置. 在每轮的最后,由最终委员会(Final Committee)计算出Randomness以供下一轮随机分片使用,随机数被广播至全网,整个网络的节点通过随机数重新计算自己所在的分片位置.

(2)基于Account模型的分片重配置. 在基于账户模型的分片系统中,分片重配置不仅涉及节点重新分配,还需要考虑账户状态的重新分区,以降低负载不均衡的风险. 例如,BrokerChain[28]提出一种工作在区块链架构协议层的账户分割机制(account segmentation mechanism),该协议将用户账户的状态划分并存储在多个分片中. 对固定状态图使用Metis(一种启发式图分区工具)进行账户分区,从而实现所有分片之间的工作负载平衡. 在每个纪元结束时,BrokerChain还需要调用布谷鸟规则(Cuckoo rule)更新M分片(Mining Shard)和P分片(Partition Shard)以防御join-leave攻击. 文献[92]提出的Transformers协议中采用了约束标签传播算法(Constrained Label Propagation Algorithm,CLPA)对整个区块链网络进行重组,通过合理控制分片的规模,来降低恶意节点对区块链系统的影响. 文献[53]提出了一个不依赖于任何安全随机数生成协议的分片重配置协议,允许每个分片独立地完成成员选择和确认过程,通过使用公共密钥哈希值进行工作量证明计算,确保了成员列表的安全性和一致性.

在重配置期间系统会变得脆弱,引起一些延迟性问题,甚至导致分片瘫痪. 在时序上,分片重配置阶段和分片建立阶段是相互衔接的. 需要说明的是,分片重配置并不意味着需要将所有的节点全部打乱,因为这意味着此阶段系统对外拒绝服务,整个系统处于停止服务的STW(Stop The World)状态. 因此,分片方案通常仅对部分节点进行打乱重组.

3.3　分片区块链的研究问题

根据上节中的分片区块链运行流程,对分片区块链的关键研究问题进行分析,以启发后续研究.

3.3.1　分片建立阶段的研究问题

(1)如何进行网络分片. 如3.2.1节所述,在网络分片阶段完成节点选择和节点分配. 节点选择是为了挑选有利于系统运行的节点. 而节点分配的任务在于通过随机性或其他手段,保证恶意节点的比例不会超过

系统以及分片的安全阈值. 网络分片面临的主要问题是51%攻击[31]. 全局来看恶意节点所占比例较低,但进行分片后,某个网络分片中恶意节点的数量超过了诚实节点的数量,可能导致该网络分片沦陷,威胁系统安全.

(2)如何完成新节点引导. 在完成节点分组后,新节点在加入各网络分片之前,需要启动引导程序,完成如下准备工作:新加入节点首先需要下载对应分片的历史数据(如账本、交易等),并获取相关配置信息,才能正常工作. 在这一过程中,恶意节点可以伪造账本数据并说服新成员作恶,从而增加恶意节点所占比例,如采用PoW共识的情况下,恶意节点说明新成员在自身分叉链上继续挖矿,增强自私挖矿攻击. 此外,如果因网络通信状况差或数据量过大等原因导致引导时间过长,新成员同步历史数据将耗费大量时间,可能造成分片无法正常工作.

(3)如何确定交易分片策略. 交易分配的策略分为随机分配策略和特定分配策略. 基于随机性的交易分配策略[12,29]简单,但会导致大量跨分片交易(如基于交易发起者地址);基于特定规则的分配策略[26,36]通过聚类、数据分析预测和交易拆分等相关技术可以减少跨分片交易的产生,但系统中的大部分交易由少量账户产生,可能导致分片中心化和分片失衡问题.

(4)如何确定内部共识协议. 在确定分片内共识策略时主要考虑以下两方面的问题:①在共识算法的可扩展性方面,需要考虑节点数量增加对分片性能的影响;②在共识算法的性能和安全性权衡方面,需要考虑共识算法和系统之间的均衡性,共识算法本身的计算开销和通信开销会影响系统的安全性和性能表现. 考虑到分片的应用初衷在于划分冲突域、降低节点负载、提升系统性能,因此分片区块链通常采用计算负载较低、通信依赖较强的BFT共识算法作为内部共识,但此类算法的性能随着节点数量增加而降低. 另外,如果需要领导者和共识委员会,在这一阶段还需要选择合适的领导者和组建初始共识委员会.

3.3.2 系统运行阶段的关键问题

(1)如何保障内部共识高效运行. 在共识算法运行时需要面临安全和性能两方面的问题. 在安全方面,需要考虑如何应对区块链常见的攻击(如自私挖矿、腐败攻击等),以及检测恶意节点和恢复沦陷分片等. 在性能方面,需要考虑如何降低分片成员之间的通信负载,方便共识协议的扩展,以及如何实现有效的共识委员会内部视图切换机制等.

(2)如何验证跨分片交易. 在进行跨分片交易过程中,交易的输入输出会涉及多个分片,需要多个分片协作完成. 共识算法的一致性将影响跨分片交易验证的复杂性. 在弱一致性共识算法中,往往需要经过后续若干区块的确认才能保证跨分片交易所涉及的区块是稳定的. 这使得跨分片交易的确认时间延长,且存在着被攻击风险,需要考虑被攻击后账本回滚的问题. 如果涉及跨分片交易的回滚,则回滚过程需要多分片协作,又将产生新的跨分片验证问题. 跨分片交易的验证策略可分为以下两类[93]:

(a)基于两阶段提交的策略(Two-Phase Commit, 2PC). 该策略由协调者收集分片委员会提供的证明并将其传输给需要的分片,通过提供的证明完成交易验证. 根据协调者的角色,基于两阶段提交的策略可分为客户端驱动的2PC、分片驱动的2PC和节点驱动的2PC. 客户端驱动的2PC,如OmniLedger[24]使用客户端软件充当协调器完成证明的收集和转发,会对客户端造成巨大开销,且客户端受网络波动影响较大,可能无法及时完成传输任务. 而且客户端缺乏账本等必要信息,无法检验证明的合法性,存在安全风险. 分片驱动的2PC需要单个或多个分片委员会协同共识,如Chainspace[35]采用输入分片作为协调者,共识开销大,对事务洪泛攻击抵抗力差,且需要提防恶意共识领导者. 节点驱动的2PC对节点要求高,如BrokerChain[28]提出经纪人账户处理跨分片交易,而经纪人需要事先抵押资产并保证账户余额充足,因此需要一定的激励措施促使节点诚实参与额外的行为.

(b)基于中继交易的策略(relay TX). 中继交易策略旨在处理跨分片的交易,确保交易的原子性和一致性. 如RapidChain[25]将原始交易拆分为多个独立的交易,每个交易仅在一个分片内处理,减少了跨分片通信的需求并保证了跨分片交易的原子性. Monoxide[29]基于提出的异步共识区采用分布式哈希表(Distributed Hash Table, DHT)和中继交易来处理跨分片交易. 通过将跨分片交易解耦为多个步骤(中继交易)并转发至目标区域,同时设计激励机制确保中继交易不会因费用分摊受到歧视,从而实现了跨区域最终原子性. 在基于中继交易的策略中,中继交易被路由至目标分片后需要后续区块的确认,导致整个跨分片交易的确认时延更长,这种时延的增加可能影响用户体验,尤其在高频交易场景下需要权衡效率与确认时延之间的平衡.

(3)如何进行新节点分配. 在某些场景中(如SSChain[30]),节点具有动态特征,可以在运行过程中自由选择某个分片加入或离开,节点的动态性将影响系统的正常运行. 在强一致性算法中,共识需要节点投票完成,而动态性意味着恶意节点的比例会不断变化. 如果诚实节点票数不足,则恶意节点成功发动攻击,导致分片沦陷. 因此,可以考虑通过节点的动态分配,控制分片内恶意节点占比.

此外,在运行过程中,可能出现分片中心化,以及分片不均衡的现象. 首先,少量用户产生系统的大部分交易,交易上的不均匀分布会导致某些分片需要处理大部分交易. 此外,随着系统的动态运行,新加入节点可能会选择加入交易较多的分片,因为这意味着更多的奖励,这可能会进一步导致分片在交易量和性能(安全性能和处理性能)上的失衡. 严重情况下,在某些分片中出现性能过剩的现象,导致不得不打包空区块,浪费系统资源.

新节点分配问题主要是针对运行过程中的不均衡. 在保证节点自由度的情况下,可以设计激励机制,确保节点的效用和系统的效用保持统一,其中节点的效用是加入某个分片获得的预期收益,系统的效用则是系统在性能上的均衡性.

(4)如何进行数据备份和恢复. 当恶意节点针对某个分片的单分片接管攻击成功,则其他分片无法依赖该分片沦陷期间提供的证明等信息完成交易验证. 因此,需要考虑维护数据存档,帮助系统恢复分片状态.

3.3.3　分片重配置阶段的问题

分片重配置发生在一个分片纪元的末期. 随着系统的不断运行,可能出现恶意节点比例接近安全阈值、分片负载均衡关系严重失调的情况. 此外,系统可以通过学习策略,基于累积数据对分片做出优化调整.

分片重配置阶段的主要任务是确定原有分片的重分配节点集合. 在这一阶段,节点选择策略分为随机替换和特定替换两种方式. 在随机替换规则中,通过可靠的随机数产生协议,对旧成员以相同概率随机替换;在特定替换规则中,出于安全和性能上的考虑,根据节点的活跃程度或者加入时间等选择替换目标,保证洗牌后的分片安全性. 随机替换策略可以为重配置后的网络提供安全性保障,但会消耗计算和通信资源,并导致系统在分片重配置阶段暂时处于停滞状态. 而特定替换的重配置方式在安全和性能之间进行权衡,既降低开销,又保证了系统的基本功能.

何时启动分片重配置是一个关键问题,因为必须保证在恶意节点成功发动攻击之前完成分片重新配置. 在文献[93]中,将该问题称为腐败时间参数的定量分析问题,其中腐败时间参数表示恶意节点完成腐败过程的时间.

3.4　分片区块链的功能组件化视角

对系统进行组件抽象有利于完善区块链分片技术协议,进而实现分片区块链的标准化开发. 受之前研究[93,94]的启发,针对3.3节提到的关键研究问题,本文进一步将其抽象为以下9个功能组件:

(1)纪元随机数生成组件. 该组件提供分片纪元内所需要的随机数.

(2)节点准入组件. 该组件负责节点选择工作,筛选有利于系统运行的节点,限制恶意节点.

(3)分片均衡组件. 不恰当的节点分配和交易分配会导致系统失衡,因此需要分片均衡组件提供安全和性能上的均衡性保障. 该组件主要包括节点分配算法、账户分配算法、交易分配算法以及均衡优化体系算法. 节点分配算法负责节点分组,实现网络分片,维持分片之间的性能均衡,保证分片安全;账户分配算法根据系统中账户的数量、活动频率以及涉及的交易复杂度进行合理的分配,有效地提高系统的整体性能和可靠性,确保分片区块链能够应对复杂的交易负载和变化的网络需求;交易分配算法实现交易分片,负责优化交易分配,降低跨分片交易数量,避免交易积压和分片闲置;均衡优化体系算法负责监视系统的平衡状态,并对交易分配和节点分片过程进行干涉.

(4)覆盖网络(Overlay Network)组件. 覆盖网络是使用网络虚拟化技术在底层网络(Underlay Network)上构建的虚拟逻辑网络,区块链的P2P网络属于一种覆盖网络. 覆盖网络组件需要提供分片之间和分片内节点之间的快速发现和路由协议.

(5)跨分片交易处理组件. 该组件处理运行过程中的跨分片交易,保证跨分片交易的原子性和效率,是实现状态分片的关键组件.

(6)激励机制组件. 该组件通过激励诚实节点,惩罚恶意节点,保证系统稳定和安全,为其他组件的运行提供支撑. 例如,为跨分片交易处理中的主要参与者提供更多奖励,或通过交易定价机制提升系统吞吐量.

(7)分片内部共识组件. 该组件提供共识协议支持,保证节点可以完成交易的验证.

(8)分片重配置组件. 该组件负责新旧节点替换、账户状态重新分区、新节点引导等工作,其他组件可以在分片重新配置期间利用本纪元生成的数据完成优化,如优化交易分配的策略、节点分配的策略和改进激励机制等.

(9)安全保障组件. 该组件为系统的安全提供保障,例如,当分片被攻击后,可以通过备份恢复进行状态回滚.

基于功能组件的分片系统结构如图7所示. 支撑性组件包括纪元随机数生成组件、覆盖网络组件、激励机制组件和安全保障组件. 纪元随机数生成组件产生随机数,为节点分配、分片重配置等流程提供随机性支撑. 覆盖网络组件构建健壮高效的P2P网络,为跨分片交易组件提供支撑,提升分片之间证明(proof)等消息的传递效率. 激励机制组件负责系统的激励设计和奖励分发,通过奖惩手段保障内部共识组件和跨分片交易组件的安全性和高效性. 分片均衡组件包括节点分配、

交易分配和均衡优化体系算法，划分系统的节点和交易，并通过均衡优化体系算法对划分流程进行干涉，保障系统的高效运行. 安全保障组件是最基本的组件，提供数据备份和恢复、状态审查和网络安全支撑等功能.

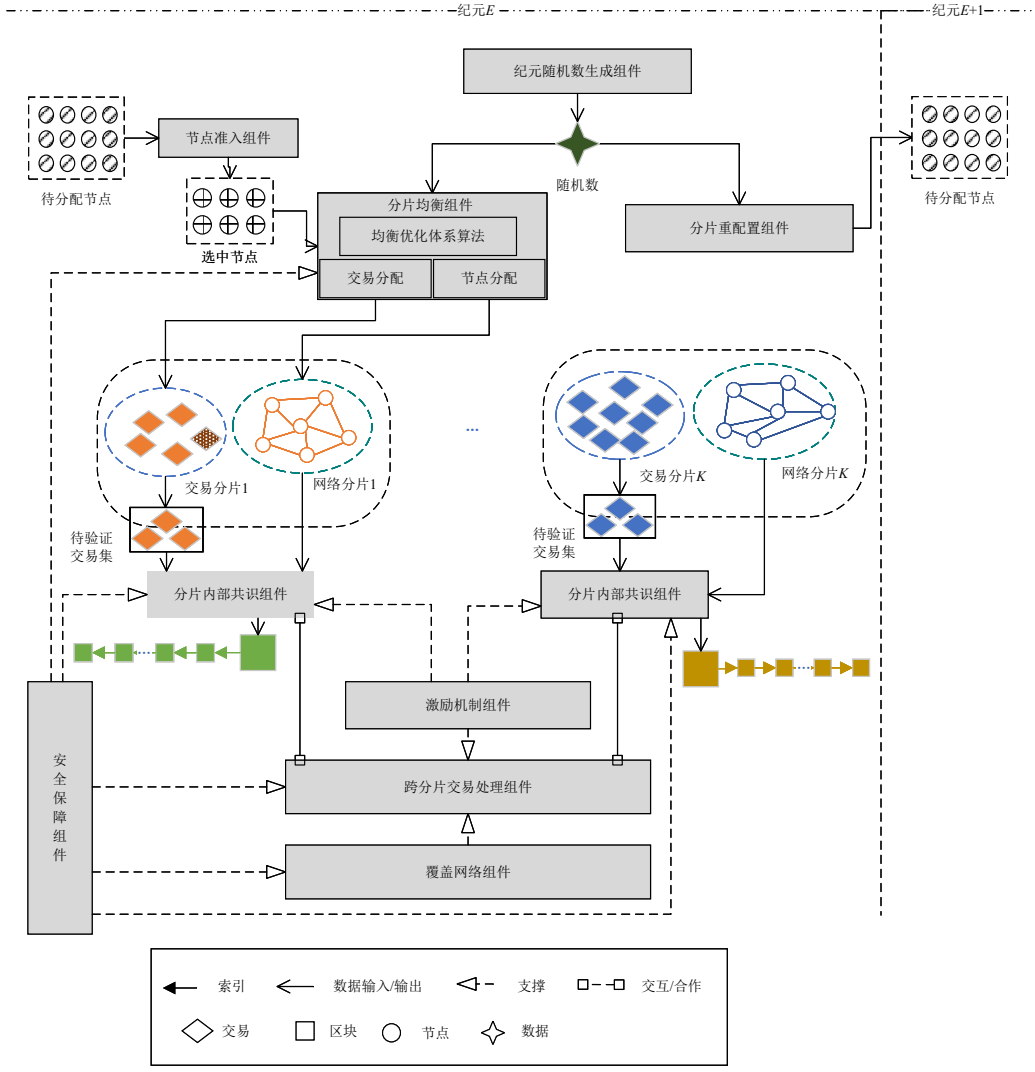


图7 基于功能组件的分片区块链

4 分片区块链现有方案分析

本章将结合3.4节提出的分片功能组件，对典型的分片区块链方案进行总结. 表1给出了基于UTXO模型的区块链分片方案，表2给出基于Account/Balance模型的区块链分片方案，表3总结了对各功能组件作出贡献的其他分片方案.

在纪元随机数生成方面，文献[39]指出传统Cointossing协议存在中心化、扩展性差和加密复杂度高的问题，提出RandGene方案通过消除复杂加密操作并引入RandChain保证安全性，但其可用性需要保证每个分片内至少存在一半的诚实节点.

节点准入环节，文献[40]发现分片区块链系统缺乏公平的节点分配机制，提出结合拜占庭容错与委托权益证明的动态分片管理方案，但该方案在分片数量激增时面临安全隐患.

网络覆盖层面，文献[104]认为传统区块链网络中的广播机制存在复杂度高、效率低下等问题，这不仅影响状态一致性，还带来了安全风险. 该研究通过改进已有的Kademlia覆盖拓扑实现高效广播，并加强了网络安全和隐私保护. 但是该研究在消息传递格式等方面仍然有改进的空间.

关于分片均衡问题，文献[42]揭示了随机分片策略虽能抵御恶意攻击，却因忽视节点差异导致性能不均衡，为此建立节点评分机制优化分配. 然而该方法仅考虑性能因素，未解决交易分配不均带来的负载压力. 文献[44]则从跨片交易角度切入，通过子交易与父交

表1　基于UTXO模型的区块链分片技术归纳

类别	区块链分片技术归纳						
分片协议	Elastico[23]	OmniLedger[24]	RapidChain[25]	OptChain[26]	RepChain[27]	SSChain[30]	Estuary[95]
数据模型	UTXO	UTXO	UTXO	UTXO	UTXO	UTXO	UTXO
纪元随机数生成	Distributed Commit-And-XOR	VRF+RandHound	DRG (Distributed Random Generation) +VSS (Verifiable Secret Sharing)	VRF+RandHound	VRF+RandHound	—	VRF
节点准入	PoW	PoW	PoW	PoW	PoW	—	PoW
分片均衡	N/A	N/A	N/A	Temporal Fitness Score	Reputation-Based Node Assignment	Market incentive Based Node Assignment	COPRAS
覆盖网络	Directory Committee	Client-Based	Kademlia-Based & IDA-Gossip	Client-Based	—	—	Kademlia-Based
跨片交易	N/A	客户端2PC	Relay TX	客户端2PC	客户端2PC	Relay TX & 分片2PC (RootChain)	节点2PC
激励机制	BR & TF (Black Reward & Transaction Fees)	BR & TF	BR & TF	BR & TF	Reputation	Market incentive	BR & TF
内部共识	PBFT	ByzCoinX	Synchronous BFT	ByzCoinX	Raft & CSBFT	PoW	PBFT & PoW
通信开销	$O(n^2)$	$O(n)$	$O(n^2)$	$O(n)$	$O(n^2)$	N/A	$O(n)$
分片重组	Shuffle	Batch	Cuckoo Rule	Cuckoo Rule	Shuffle	N/A	Cuckoo Rule
安全保障	基于最终委员会	—	—	—	—	基于根链结构	—
弹性	$n/4$	$n/4$	$n/3$	$n/4$	$n/3$	$n/4$	$n/3$

注:n:区块链规模大小(节点数);—:没有明确指出;弹性值来自原始论文,定义见2.1节.

易同分片的分配策略减少跨片交易,并实现交易均衡分配,却忽视了节点性能差异对吞吐量的制约.

在分片内部共识机制上,文献[52]指出了现有分片区块链内部共识协议中,拜占庭容错协议安全保证不足,其他强共识协议又存在恶意节点容忍度低的问题. 该文献提出的MWPoW+协议在容忍半数恶意节点的同时能够确保安全,但带来了较高的时间复杂度和额外的投票链维护成本.

跨分片交易处理方面,文献[47]针对物联网场景下计算成本过高的情况,采用改进的KZG承诺(Kate-Zaverucha-Goldberg Commitment)聚合方法降低计算难度,但未涉及其他性能维度的优化.

激励机制方面,文献[48]指出了现有区块链系统缺乏监督机制的问题,并将博弈论引入激励机制设计,通过合作博弈实现系统自我审计,但未考虑恶意节点可能采取的非理性策略.

在分片重配置阶段,文献[113]发现Merkle树的状态存储因数据迁移和树重构产生巨大网络与计算开销,限制系统扩展性. 研究采用一致性哈希减少迁移,用Merkle B+树降低重构成本,确保迁移时服务可用,但未解决新节点引导问题.

最后从安全保障角度,文献[115]针对恶意的交易分配策略,采用李雅普诺夫优化方法,不仅能有效抵御bursty-TX注入攻击,还优化了交易分配. 然而,这种防御策略的应用范围存在局限性,仅适用于防范特定类型的拥塞攻击.

根据分片区块链的架构,可以将上述研究成果分为3类:

(1)扁平化的单层架构. 在扁平化的架构中,所有分片的职能和地位是相同的. 每个分片都独立地完成交易验证、区块打包等操作. 大部分方案都是单层架构,如OmniLedger、RapidChain、OptChain、RepChain等.

(2)层次化的多层架构. 层次化的多层架构设计的目的在于,让不同的分片承担不同的职能,以此提升性能或安全. 例如Elastico采用了最终委员会和普通委员会双层架构;SSChain使用根链和分片链处理不同事务;BrokerChain设计了P分片和M分片;Monoxide、Ethereum 2.0也是类似的双层架构. AMC设计了3种不同职能的分片. 多层架构优点是可以解决跨分片交易的验证问题,但分片之间是完全隔离的非重叠结构,因此需要增加额外开销保证跨分片交易的原子性和一致性,这降低了分片的性能[55]. 除此以外,还需要设计相

表2 基于Account/Balance模型的区块链分片技术归纳

类别	区块链分片技术归纳					
分片协议	BrokerChain[28]	Monoxide[29]	Ethereum 2.0[31]	AMC[32]	CoChain[96]	LB-Chain[97]
数据模型	Account/Balance	Account/Balance	Account/Balance	Account/Balance	Account/Balance	Account/Balance
纪元随机数生成	—	—	RANDAO+VDF (Verifiable Delay Function)	MPC (Multi-Party Compution)	VRF+VDF	—
节点准入	PoW	—	Deposit	Deposit	PoW	—
分片均衡	State Partition and Account Segmentation	N/A	—	N/A	N/A	Account and Transaction Migration
覆盖网络	Kademlia-Based	Gossip	—	—	Kademlia-Based	Gossip
跨片交易	节点2PC (BrokerAccount)	Relay TX	分片2PC (BeaconChain)	—	节点2PC	Relay TX
激励机制	BR & TF	BR & TF based Chu-ko-nu Mining	BR & TF	Deposit based	BR & TF	BR & TF
内部共识	PBFT	PoW-based GHOST[17]	PoS-based Casper FFG	PoS-based improved Tendermint	BFT	PoW
通信开销	$O(n^2)$	N/A	$O(n^2)$	$O(n^2)$	$O(n^2)$	N/A
分片重组	Cuckoo Rule	—	—	Shuffle	VRF+VDF	Cuckoo rule and distributed randomness generation scheme
安全保障	—	基于Global Swarm	基于信标链	基于聚合分片	基于pipelining mechanism	Dynamic Load Balancing
弹性	$n/2$	$n/2$	$n/3$	$n/3$	$n/3$	$n/2$

注：n：区块链规模大小(节点数)；—：没有明确指出；弹性值来自原始论文，定义见2.1节.

应的激励机制，鼓励部分节点承担额外的工作.

(3)分层融合架构. 在分层融合架构中，分片之间并不是完全割裂的，某些节点可以同时存在于多个分片. 文献[55]提出金字塔分层融合架构，允许某些节点同时参与多个分片的运行，这些节点组成的分片可以存储多个分片的完整记录，可以作为特定分片之间的跨分片交易处理中介. 此外，BrokerChain允许部分普通用户通过抵押资产成为“经纪人账户”，而经纪人账户状态会被分配到多个分片中，参与多个跨分片交易的协调，因此也可归属于分层融合架构.

5 分片技术面临的挑战和展望

5.1 研究挑战

分片方案的核心挑战是在不牺牲系统安全性和去中心化的前提下，尽可能地提升系统性能. 下面给出分片技术面临的主要挑战.

5.1.1 安全方面

基于分片的区块链方案在安全方面的挑战主要来源于共识协议、随机数生成、跨分片交易处理方案、激励机制和安全保障机制.

共识协议作为系统运行的基石，共识安全性很大程度上决定了系统的安全性. 基于PoW的共识及改进方案可以提供较强的安全性，但基于PoW的共识使得节点存在激烈的竞争，节点为了获得出块权需要具有独立执行和验证交易的能力，因此需要存储全局数据，节点存储开销大. 未来需要考虑如何在避免高存储开销的前提下维持基于PoW共识方案的安全性. 对于基于BFT的共识，通过牺牲部分安全性来换取系统性能的提升. 在这样的方案中，需要在其他方面特别地进行安全设计，如优化随机数生成组件实现更安全的随机性、通过激励方案强化协作和抵抗恶意节点，或者优化共识协议提升安全性等.

跨分片交易处理方案的安全挑战在于如何保证交易的状态一致性和原子性. 在现有的大部分方案中，跨分片交易的处理过程需要节点间的交互，这意味着需要考虑节点恶意的行为. 针对跨分片交易的安全性问题，不同方案提出了各自的策略. 例如，X-Shard[108]通过引入由分片委员会管理的网关账户机制，将跨分片交易验证分解为多个分片内验证，采用阈值签名技术防止恶意节点伪造有效签名，并结合回滚机制来确保

表3　针对组件贡献总结的其余相关研究

组件		相关参考文献	突出贡献
纪元随机数生成		文献[39]	Randchain设计并实现了实用可扩展的分布式随机数生成协议
节点准入		文献[40]	基于PoS实现公平的节点选择
		文献[41]	Sharper在许可链中采用CA(Certificate Authority)选择参与节点
分片均衡	节点分配策略	文献[36]	根据智能合约的调用历史进行节点分配
		文献[42]	NRSS对节点评级,根据平衡分数进行节点分配,减少分配之间的性能差异
		文献[42]	GeoChain对节点的物理特征和位置进行聚类,从而形成分片
		文献[97]	通过基于机器学习的预测结果运行账户迁移算法,动态平衡不同分片上的交易负载
		文献[98]	计算最佳放置并决定跨分片的对象迁移,利用调度器平衡分片之间的负载并改进了数据局部性
		文献[99]	采用社区检测方法划分账户,改善分片区块链的吞吐量和交易时延
		文献[100]	提出NACV(Node Allocation algorithm based on node Contribution Values)算法,基于动态节点贡献值(性能与安全)优化节点分配,减少压力差异,平衡分片处理能力与负载
	交易分配策略	文献[44]	基于交易和历史交易的交互,利用图论知识实现交易的智能放置,减少跨片交易数量以及对系统性能的影响
		文献[101]	提出链下实时迁移方法来减少链上交易的数量,提高平衡过程中的效率和可用性
		文献[102]	采用Blob-carrying交易来分离TX的执行与数据的存储,允许Rollup将批量交易数据存入Blob,降低主链负担
覆盖网络		文献[45]	Ostraka实现分布式节点结构,对节点分片
		文献[103]	DASH(DAG-based blockchain SHarding)是针对6G网络设计的方案,将分片和DAG技术结合
		文献[104]	结合QUIC(Quick UDP Internet Connections)协议改进已有的Kademlia覆盖拓扑,降低复杂度的同时避免网络拥塞
跨分片交易		文献[46]	改进Polyshard的编码分片方案;使用分布式存储支持块传播,改善传播延迟
		文献[47]	提出新的数据结构,对跨分片交易的大小压缩,从而提升跨分片通信效率
		文献[96]	将参与跨分片交易的分片通过分布式协议共同协调和验证交易的执行,高度去中心化,较高并行性与吞吐量
		文献[105]	引入编排执行模型(Orchestration Execution Model,OEM),在Byzantine环境中高效地实现两阶段提交和两阶段锁定
		文献[106]	利用中继链上交易的依赖性将具有依赖性的交易放到一个分片中,从而消除跨分片交易
		文献[107]	基于跨分片节点合作与无状态排序确定全局交易执行顺序,从而避免跨分片交易冲突
		文献[108]	提出一种乐观策略处理多输入多输出(Multiple-Input Multiple-Output,MIMO)的跨分片交易,通过建立网关账户,在分片内处理跨分片交易的子交易,减少交易处理延迟
		文献[109]	CHERUBIM在传统两阶段提交(2PC)的基础上,引入了四重管道两阶段提交(Quadruple Pipelined Two-Phase Commit,4P-2PC)方法,提高跨分片交易的并行处理能力,减少交易提交过程中的等待时间
激励机制	基于现有激励模型	文献[48]	利用合作博弈的两阶段讨价还价模型,得到交易和奖励分配的最佳方式
		文献[49]	分析了共识领导者在分配奖励中的博弈行为,研究该行为对其他共识节点的影响
	基于新的激励模型	文献[36]	基于智能合约实现;提出分片奖励(ShardReward),鼓励小分片合并
		文献[50]	提出RepShard,采用声誉作为激励
		文献[51]	在契约理论的框架下,通过设计合理保证金,平衡安全和经济激励的问题
		文献[110]	首次设计激励机制鼓励用户成为代理人,允许Broker在跨分片交易中得到佣金奖励
内部共识		文献[33]	Logos采用Axios共识,这是PBFT的委托版本
		文献[37]	ZILLIQA是第一个采用分片和PoW的分片协议;支持去中心化应用(decentralized Application,dAPP)
		文献[52]	提出基于投票的MWPoW+协议,用于强共识,可容忍最多$f<n/2$个恶意节点
		文献[111]	采用BABE/GRANDPA混合共识,BABE(Blind Assignment for Blockchain Extension)负责产生分片区块并确保其活性,GRANDPA(GHOST-based Recursive Ancestor Deriving Prefix Agreement)保证账本一致性
分片重配置		文献[53]	是第一个不依赖于任何安全随机数生成协议的分片重配置协议,适用于基于委员会的分片区块链
		文献[54]	提出SRB(Secure-Repair-Blockchain)协议,采用编码理论技术,减少传输数据量,降低引导成本
		文献[112]	利用一致性哈希分配账户,从而减少分片重配置时分片数量改变导致的数据迁移
		文献[113]	提出新的MPT树(tMPT),提高同步状态数据的效率;提出基于tMPT的分片重组协议
安全保障		文献[36]	提出"MaxShard"结构,存储全局信息
		文献[114]	提出一个双链架构,将出块和区块共识解耦,从而允许在共识期间跨分片合作
		文献[115]	提出一种自适应资源分配算法,为每个网络分片提供近乎最优的解决方案,同时分片队列也能得到稳定的维护,抵御交易突发注入攻击

交易安全性与状态一致性. 又例如,Sharon[116]采用分片成对合并的方式处理跨分片交易,该方法能够有效防范恶意节点利用分片间通信延迟发起的双花攻击,同时避免了传统跨片交易回滚的高复杂度,保证跨片交易的原子性,从根源上解决了潜在的跨片交易安全问题. 基于智能合约的方案也是一种可行的解决思路[117]. 目前有文献[35]和文献[38]等方案提出了基于锁的跨分片共识协议,以便使用智能合约处理跨分片交易. 为了保证原子性和一致性,所有涉及的数据都在跨分片共识过程中被锁定. 虽然这种方式会增加交易延迟,但其影响仍在可接受范围内.

激励机制是分片方案的重要组件,合理的激励机制可以激励系统节点做出诚实且有利于系统发展的行为,增加对恶意节点的抵抗能力,这对系统安全尤为重要. Broker2Earn[110]设计了一个激励机制鼓励用户成为代理人,但匹配方式可能存在的资源浪费,设计的算法也可能导致某些节点操纵市场. 诸多文献分析激励机制下节点之间的博弈行为,通过理解节点的博弈,可以促进激励机制的改进.

安全保障机制主要针对系统故障后如何恢复的问题. 一种方案是从存储方面入手,如采用链下存储,当链上数据出错,通过链下备份恢复链上的状态. 但该方法将安全风险转移到链外,需要考虑新的攻击行为. 另一种方案是在系统中设计存储全局状态的结构,此类结构往往需要具有很强的抗风险能力,如SSChain的根链结构,但这种解决方案需要节点具有较强的存储能力,也会导致系统的可扩展能力变差.

5.1.2 性能方面

基于分片的区块链方案在性能方面的挑战主要来自共识协议和跨分片交易处理方案. 在依赖通信的共识协议中,共识协议的通信复杂度、视图切换的复杂度都直接影响着系统的性能表现. 如以PBFT为代表的一类共识,通信复杂度高,这使得系统的扩展性差,当系统节点超过100时,系统的性能明显变差.

跨分片交易是分片方案的独有部分,需要多分片协同验证,增加了通信开销,降低系统的整体吞吐量和响应速度. OmniLedger采用了2PC协议来保证跨分片交易的原子性和一致性. 虽然这种方案可以确保安全性,但由于多轮次的通信和协调,它的延迟较高,限制了吞吐量. RapidChain使用relay TX来减少跨分片交易的延迟和通信开销. 然而,随着分片数量的增加,系统仍然需要协调多个分片之间的状态更新,无法完全避免跨分片交易的影响.

5.1.3 均衡性方面

在基于分片技术的区块链系统中,分片失衡会影响系统的运行效率. 中心化问题会导致分片失衡. 首先,由于交易是由系统用户发布的,而实际上系统中的大部分交易是由少部分用户发布的,这些交易之间存在很大的相关性. 如果基于交易双方来决定交易的验证分片,那么可能导致某些分片需要处理过量的交易;而如果对交易进行随机分配,那么可能导致跨分片交易的泛滥,而验证跨分片交易又是复杂的. 此外,系统中的验证者并非完全对等的,某些节点具有优越的算力和通信资源,甚至节点持有者在现实世界中的声望也会影响区块链世界的运行. 对于这类节点的处理需要谨慎进行,如果节点分配策略失当,就会导致分片之间在处理性能上出现失衡. 此外,从现实角度来看,在地理位置上亲近的节点之间很有可能形成较为亲密的组织,而能力较弱的节点也可能会抱团形成矿池,需要分析这些行为对系统均衡性的影响,并寻找相应的解决方案.

从目前的解决方案来看,保证分片系统的均衡性主要从降低跨分片交易数量、维持分片之间交易数量和处理性能平衡等几个方面出发. 基于声誉可以有效地量化性能,但不同的系统对于声誉的定义也不一致. 此外,网络状态是随机变化的,这种不确定性会导致系统运行状态的波动性. 文献[10]表明分片规模与网络安全之间存在关联:当分片规模变大,失败概率降低,失败年限增加,但相应的通信开销会增加. 维护系统的高安全级别往往带来较大的开销,因此需要动态调整系统均衡性指标,在安全和性能之间找到一个平衡. 目前来看,均衡性的定义以及评价指标并没有在研究界达成一致,对于动态均衡的相关研究仍然欠缺.

5.2 研究展望

为了应对上述挑战,本文从功能组件角度对未来分片区块链开发流程和仿真进行展望,并讨论了分片技术与其他扩展技术融合.

(1)标准化分片区块链开发流程

分片技术的标准化将有效促进分片区块链的发展,本文探索了功能组件视角开发分片区块链的流程,表4给出了各功能组件的设计目标. 表5和表6分别总结了各种分片方案在不同的分片规模下的吞吐量和时延. 根据表5的数据显示,目前在吞吐量方面表现最好的分片技术Estuary在分片规模32的情况下达到了11 850.4 TPS,但支付宝的日常平均吞吐量达到50 000 TPS以上. 根据表6数据显示,目前在时延方面表现最好的分片技术OptChain在分片规模6的情况下达到了6.6 s,满足了大多数主流支付系统对时延的要求,但在该分片规模下吞吐量仅达到1 200 TPS. 目前分片方案的性能与现实应用场景的需求仍然存在一定差距,需要后续从不同功能组件角度进行深入研究,提高分片区块链的性能.

表4　功能组件角度的设计目标

组件	设计目标
纪元随机数生成组件	随机数生成算法需要满足公开可验证、不可预测、抗偏置、可用性
节点准入组件	提高恶意节点的准入成本
覆盖网络组件	实现快速路由和节点发现;设计更健壮的拓扑结构
分片均衡组件	避免单点过热;考虑动态维持均衡问题
分片内部共识组件	减少通信开销;提升安全性
跨分片交易处理组件	减少跨分片交易数量;简化处理流程;提升安全性
激励机制组件	激励诚实节点,惩罚恶意节点,保证系统稳定和安全
分片重配置组件	减少节点存储开销,提高账本迁移率
安全保障性组件	考虑链外存储,保证数据安全性

表5　不同分片协议在吞吐量方面的性能　　单位:TPS

分片数量/个	2	4	6	8	16	32
OmniLedge	869(70)	1 674(70)	—	3 240(70)	5 850(70)	—
RapidChain	—	1 750(145)	2 744(175)	3 726(190)	7 384(250)	—
OptChain	—	—	1 200(400)	2 700(400)	6 500(400)	—
RepChain	1 834(225)	3 610(225)	5 333(225)	6 853(225)	—	—
Estuary	786.2(39)	1 511.9(57)	—	2 910.5(69)	6 093.2(81)	11 850.4(87)
BrokerChain	—	—	—	1 250(14)	1 700(7)	2 500(3)
Monoxide	25(24 000)	42(12 000)	—	80(6 000)	160(3 000)	200(1 500)
CoChain	—	579(500)	737(550)	887(575)	—	—
LB-Chain	—	229(64)	—	395(32)	750(16)	1 450(8)

注:“—”表示没有明确指出;括号内的数据表示每个分片内节点的数量;该数据来源于原始论文.

表6　不同分片协议在时延方面的性能　　单位:s

分片数量/个	2	4	6	8	16	32
OmniLedge	9.9(70)	9(70)	9.3(70)	—	—	—
RapidChain	—	8.04(145)	8.49(175)	8.64(190)	8.84(250)	—
OptChain	—	—	6.6(400)	7.2(400)	10.5(400)	—
RepChain	—	146(450)	88.5(300)	58.2(225)	—	—
Estuary	—	—	—	—	7(81)	—
BrokerChain	—	—	—	370(14)	130(7)	55(3)
Monoxide	12(24 000)	13.5(12 000)	—	14.5(6 000)	15(3 000)	15(1 500)
CoChain	—	34(500)	35(550)	36(575)	—	—
LB-Chain	—	35(64)	—	120(32)	60(16)	125(8)

注:“—”表示没有明确指出;括号内的数据表示每个分片内节点的数量;该数据来源于原始论文.

(2)将分片技术与其他扩展技术融合

2.2节结合区块链的逻辑结构,阐述了扩展区块链的思路.在未来的可扩展性研究中,可以考虑在分片的基础上再次分片的“超二次分片”,或者考虑自适应的动态分片策略,通过智能合约实现按需创建和关闭分片,并通过跳跃哈希等方式减少节点和数据变动.此外,未来的工作中可以将分片技术与其他可扩展技术结合,例如将支付通道和链上分片方案进行组合,通过智能合约和抵押等方式,委托那些使用支付通道的节点通过链下支付处理链上跨分片交易.

在交易分片方面,诸多研究工作利用社区划分等算法,基于历史信息进行交易分配,在减少跨分片交易的方面颇有成效.但此类算法需要纪元运行的历史数据,且难以对当前纪元的交易分配过程做出及时的反应.在未来的工作中,可以考虑利用深度学习等工具,通过对交易特征的学习,预测其分配结果,从而实现实时的交易分配优化.

在共识方面,分片区块链一般直接采用现有的共识方案,因此底层共识的研究很大程度上决定了分片区块链的共识性能.但分片区块链技术的关键在于牺牲安全换取性能,针对具体的应用场景,分片区块链技

术对于共识的选择应该更加灵活,在共识节点选择、通信交互等方面可以采用更加大胆的策略.

在状态分片方面,账本数据迁移一直是需要解决的难题,为了保证区块链系统的安全性,现有的迁移协议通常利用锁机制将迁移账本的所有交易锁定在源分片中(如LB-Chain[97]等),导致交易确认时延较长. 部分方案在此基础上进行改良,如Fine-tune Lock[118]方案仅锁住扣款操作的交易而允许收款交易继续执行,但扣款交易的确认时延较长,对区块链系统的吞吐量也会造成一定程度上的影响. 对此可以考虑通过代理人机制专门处理账本锁定中发生的交易来缩短交易时延并提高吞吐量,具体迁移流程如图8所示.

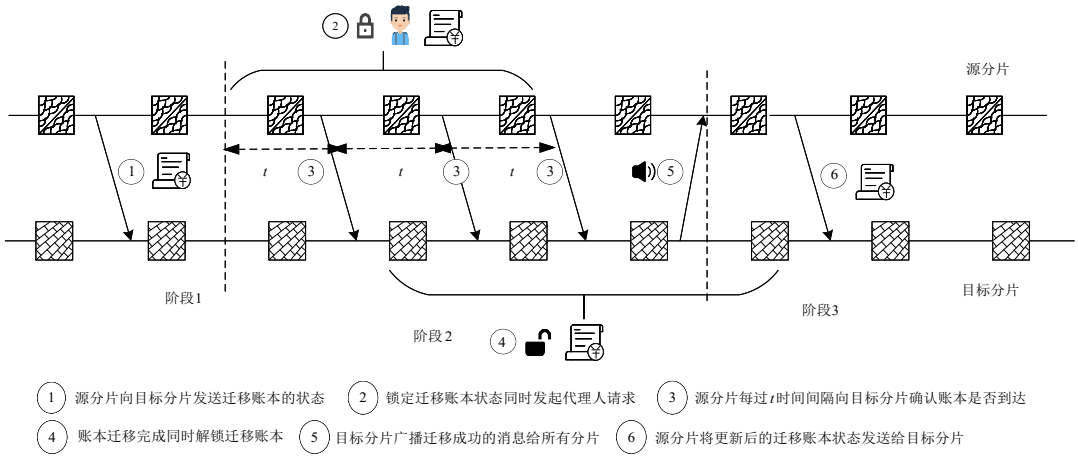


图8 基于代理人的账本迁移机制

在基于代理人的账本迁移机制中,源分片首先向目标分片发送待迁移账本状态并锁定迁移账本. 随后,代理人直接接管被锁定账本的交易处理,确保交易持续处理,并参考TCP/IP协议三次握手的通信过程,源分片每隔t时间间隔向目标分片发送确认信息. 迁移成功完成后,目标分片广播迁移完成消息并解锁账本. 最后,源分片向目标分片发送账本更新后的状态.

上述的解决方案虽然可以有效提高系统吞吐量,但代理人角色的诚实度也显得更加重要,而现有MPT树结构缺乏对应的信誉值评估机制,难以有效识别并选取诚实节点作为代理人,这会带来系统安全性隐患,因此还需对MPT树结构进行改进. 考虑在MPT树的基础上,新增“Reputation”字段以记录节点的信誉评分(如图9),通过信誉评分与质押机制结合,可以有效约束代理人行为,减少恶意节点的作恶动机,提高系统整体安全性,同时信誉值高的节点可以获得更多代理机会,提高收益,形成良性竞争,优化资源分配.

为了优化区块链存储效率,研究团队着眼于采用具备高效检索特性的学习索引技术,例如,文献[119]提出创新性的列式学习存储架构COLE,通过深度融合学习索引,采用异步合并算法,最终构建起支持多维查询的高效存储体系,在保障区块链核心特性的同时实现存储性能的全面提升.

尽管学习索引技术可压缩存储,但其在分片场景下面临三重挑战:其一,跨分片查询需多次网络通信,动态分片边界变化使得学习索引模型难以实时适配,

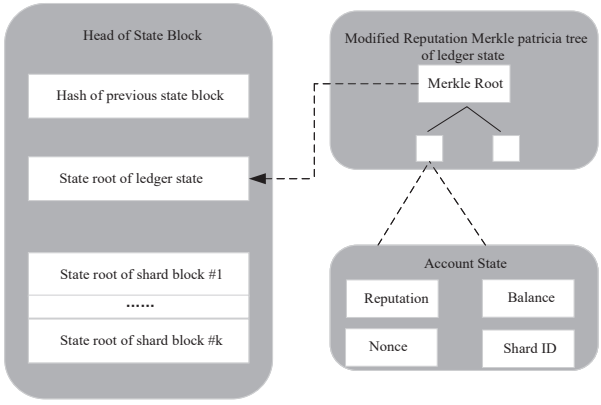


图9 基于信誉值的MPT树结构

导致跨分片定位效率低下;其二,跨片交易需聚合多分片生成的Merkle证明,验证复杂度随分片数量线性攀升;其三,分片合并或分裂时需全量重构索引,不仅产生较高的延迟,更破坏存储连续性,导致后续查询性能骤降. 这些瓶颈严重制约了分片区块链的扩展性与实用性.

针对上述问题,可以考虑优化的列式学习存储架构,每个分片独立部署COLE实例,按地址连续存储状态历史版本,构建全局轻量级学习索引,减少跨片查询跳数. 分片合并时,基于列式存储的物理连续性直接拼接数据块,避免索引重构;分片分裂时,子分片继承父分片学习模型并增量训练,使之适用于分片区块链存储.

(3)开发通用的分片区块链仿真平台

BlockEmulator[120]提供了多种共识协议与跨分片机

制(Monoxide 和 BrokerChain)的区块链协议验证机制,为开发通用的分片区块链仿真平台提供了基础. 未来可以设计一套配置简单、用户友好的通用分片区块链仿真平台,以组件模块方式实现上述提到的组件功能函数,并提供不同组件的二次开发接口,减小分片区块链研究和开发成本.

6 结束语

可扩展性是影响区块链技术被广泛应用的障碍之一,分片技术为其提供了可行的解决方案. 本文首先结合区块链逻辑层级对区块链可扩展性方案进行总结,然后重点关注分片方案. 本文从不同的视角对分片区块链进行概述,总结分析了分片区块链的结构层次、运行流程和关键研究问题,接着从功能组件角度总结了分片区块链的研究现状,最后分析了分片区块链研究的挑战以及未来的研究方向. 随着分片区块链技术的发展,将加快区块链应用场景向纵深发展,进一步释放区块链技术的潜在价值.

参考文献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2021-12-01) [2025-05-02]. https://bitcoin. org/bitcoin.pdf.

[2] 蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术[J]. 计算机学报, 2021, 44(1): 84-131.
CAI X Q, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131. (in Chinese)

[3] 唐飞, 冯卓, 黄永洪. 基于区块链的公平可验证数据持有方案[J]. 电子学报, 2023, 51(2): 406-415.
TANG F, FENG Z, HUANG Y H. Fair provable data possession scheme based on blockchain[J]. Acta Electronica Sinica, 2023, 51(2): 406-415. (in Chinese)

[4] ROCHA G D S R. DE OLIVEIRA L, TALAMINI E. Blockchain applications in agribusiness: A systematic review[J]. Future Internet, 2021, 13(4): 95.

[5] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: Principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151. (in Chinese)

[6] GERVAIS A, KARAME G O, WÜST K, et al. On the security and performance of proof of work blockchains[C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 3-16.

[7] SCHÄFFER M, DI ANGELO M, SALZER G. Performance and scalability of private ethereum blockchains[C]//Business Process Management: Blockchain and Central and Eastern Europe Forum. Cham: Springer, 2019: 103-118.

[8] YU G S, WANG X, YU K, et al. Survey: Sharding in blockchains[J]. IEEE Access, 2020, 8: 14155-14181.

[9] ZHOU Q H, HUANG H W, ZHENG Z B, et al. Solutions to scalability of blockchain: A survey[J]. IEEE Access, 2020, 8: 16440-16455.

[10] HAFID A, HAFID A S, SAMIH M. Scaling blockchains: A comprehensive survey[J]. IEEE Access, 2020, 8: 125244-125262.

[11] NASIR M H, ARSHAD J, KHAN M M, et al. Scalable blockchains: A systematic review[J]. Future Generation Computer Systems, 2022, 126(C): 136-162.

[12] CROMAN K, DECKER C, EYAL I, et al. On scaling decentralized blockchains: (a Position Paper)[M]//Financial Cryptography and Data Security. Berlin: Springer, 2016: 106-125.

[13] KLARMAN U, BASU S, KUZMANOVIC A, et al. BloXroute: A scalable trustless blockchain distribution network whitepaper[EB/OL]. (2018-03-28) [2025-05-02]. https://bloxroute. com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf.

[14] ROHRER E, TSCHORSCH F. Kadcast: A structured approach to broadcast in blockchain networks[C]//Proceedings of the 1st ACM Conference on Advances in Financial Technologies. New York: ACM, 2019: 199-213.

[15] MAO Y F, DEB S, VENKATAKRISHNAN S B, et al. Perigee: Efficient peer-to-peer network design for blockchains[C]//Proceedings of the 39th Symposium on Principles of Distributed Computing. New York: ACM, 2020: 428-437.

[16] CORALLO M. Bip152: Compact block relay[EB/OL]. (2016-04-01)[2025-05-02]. https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki.

[17] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in Bitcoin[C]//Financial Cryptography and Data Security. Berlin: Springer, 2015: 507-527.

[18] LI C X, LI P L, ZHOU D, et al. Scaling akamoto onsensus to thousands of transactions per second[EB/OL]. (2018-08-31)[2025-05-02]. http://arXiv:1805.03870.

[19] CUI L Z, YANG S, CHEN Z T, et al. An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2019, 16(6): 4134-4145.

[20] POPOV S, MOOG H, CAMARGO D, et al. The coordicide[EB/OL]. (2020-01-01)[2025-05-02]. http://files.iota.org/papers/20200120_Coordicide_WP.pdf.

[21] 孙知信, 张鑫, 相峰, 等. 区块链存储可扩展性研究进展[J]. 软件学报, 2021, 32(1): 1-20.
SUN Z X, ZHANG X, XIANG F, et al. Survey of storage scalability on blockchain[J]. Journal of Software, 2021, 32(1): 1-20. (in Chinese)

[22] ABE R, SUZUKI S, MURAI J. Mitigating Bitcoin node storage size by DHT[C]//Proceedings of the Asian Internet Engineering Conference. New York: ACM, 2018: 17-23.

[23] LUU L, NARAYANAN V, ZHENG C D, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 17-30.

[24] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger: A secure, scale-out, decentralized ledger via sharding[C]//2018 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2018: 583-598.

[25] ZAMANI M, MOVAHEDI M, RAYKOVA M. RapidChain: Scaling blockchain *via* full sharding[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 931-948.

[26] NGUYEN L N, NGUYEN T D T, DINH T N, et al. OptChain: Optimal transactions placement for scalable blockchain sharding[C]//2019 IEEE 39th International Conference on Distributed Computing Systems. Piscataway: IEEE, 2019: 525-535.

[27] HUANG C Y, WANG Z Y, CHEN H X, et al. RepChain: A reputation-based secure, fast, and high incentive blockchain system via sharding[J]. IEEE Internet of Things Journal, 2021, 8(6): 4291-4304.

[28] HUANG H W, PENG X W, ZHAN J Z, et al. BrokerChain: A cross-shard blockchain protocol for account/balance-based state sharding[C]//IEEE INFOCOM 2022 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2022: 1968-1977.

[29] WANG J, WANG H. Monoxide: Scale out blockchains with asynchronous consensus zones[C]//USENIX Symposium on Networked Systems Design and Implementation (NSDI 19). Boston: USENIX Association, 2019: 95-112.

[30] CHEN H, WANG Y J. SSChain: A full sharding protocol for public blockchain without data migration overhead[J]. Pervasive and Mobile Computing, 2019, 59: 101055.

[31] BUTERIN V. Ethereum Sharding FAQs[EB/OL]. (2022-09-28)[2025-05-02]. https://github.com/ethereum/wiki/wiki/Sharding-FAQs.

[32] WANG M N, JIANG Y H, HUANG J H, et al. AMC: A PoS blockchain consensus protocol for scalable nodes[J]. International Journal of Network Security, 2022, 24(5): 802-814.

[33] ZOCHOWSKI M. A Highly Scalable Decentralized Transaction System[EB/OL]. (2018-02-28)[2025-05-02]. https://logos.network/whitepaper.pdf.

[34] DANG H, DINH T T A, LOGHIN D, et al. Towards scaling blockchain systems via sharding[C]//Proceedings of the 2019 International Conference on Management of Data. New York: ACM, 2019: 123-140.

[35] Al-BASSAM M, SONNINO A, BANO S, et al. Chainspace: A sharded smart contracts platform[EB/OL]. (2017-08-12)[2025-05-02]. https://arxiv.org/pdf/1708.03778.

[36] TAO Y C, LI B, JIANG J J, et al. On sharding open blockchains with smart contracts[C]//2020 IEEE 36th International Conference on Data Engineering. Piscataway: IEEE, 2020: 1357-1368.

[37] ZILLIQA Team. The ZILLIQA technical whitepaper[EB/OL]. (2017-09-16)[2025-05-02]. https://docs.zilliqa.com/whitepaper.pdf.

[38] HARMONY Team. Harmony technical whitepaper[EB/OL]. (2023-02-28)[2025-05-02]. https://harmony.one/whitepaper.pdf.

[39] WANG G, NIXON M. RandChain: Practical scalable decentralized randomness attested by blockchain[C]//2020 IEEE International Conference on Blockchain. Piscataway: IEEE, 2020: 442-449.

[40] LEE D R, JANG Y, KIM H. Poster: A proof-of-stake (PoS) blockchain protocol using fair and dynamic sharding management[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2019: 2553-2555.

[41] AMIRI M J, AGRAWAL D, EL ABBADI A. SharPer: Sharding permissioned blockchains over network clusters[C]//Proceedings of the 2021 International Conference on Management of Data. New York: ACM, 2021: 76-88.

[42] WANG J R, ZHOU Y, LI X W, et al. A node rating based sharding scheme for blockchain[C]//2019 IEEE 25th International Conference on Parallel and Distributed Systems. Piscataway: IEEE, 2019: 302-309.

[43] MAO C Y, GOLAB W. GeoChain: A locality-based sharding protocol for permissioned blockchains[C]//Pro-

ceedings of the 24th International Conference on Distributed Computing and Networking. New York: ACM, 2023: 70-79.

[44] REN L Y, WARD P A S, WONG B. Toward reducing cross-shard transaction overhead in sharded blockchains[C]//Proceedings of the 16th ACM International Conference on Distributed and Event-Based Systems. New York: ACM, 2022: 43-54.

[45] MANUSKIN A, MIRKIN M, EYAL I. Ostraka: Secure blockchain scaling by node sharding[C]//2020 IEEE European Symposium on Security and Privacy Workshops. Piscataway: IEEE, 2020: 397-406.

[46] WANG C R, RAVIV N. Low latency cross-shard transactions in coded blockchain[C]//2021 IEEE International Symposium on Information Theory. Piscataway: IEEE, 2021: 2678-2683.

[47] KUDZIN A, TOYODA K, TAKAYAMA S, et al. Scaling ethereum 2.0s cross-shard transactions with refined data structures[J]. Cryptography, 2022, 6(4): 57.

[48] KIM S. Two-phase cooperative bargaining game approach for shard-based blockchain consensus scheme[J]. IEEE Access, 2019, 7: 127772-127780.

[49] HEMATI M, SHAJARI M. An incentive compatible reward sharing approach for shard-based blockchains[C]// 2021 29th Iranian Conference on Electrical Engineering. Piscataway: IEEE, 2021: 526-532.

[50] WANG G. RepShard: Reputation-based sharding scheme achieves linearly scaling efficiency and security simultaneously[C]//2020 IEEE International Conference on Blockchain. Piscataway: IEEE, 2020: 237-246.

[51] LI J, LIU T T, NIYATO D, et al. Contract-theoretic pricing for security deposits in sharded blockchain with Internet of Things (IoT)[J]. IEEE Internet of Things Journal, 2021, 8(12): 10052-10070.

[52] XU Y B, SHAO J H, SLAATS T, et al. MWPoW+: A strong consensus protocol for intra-shard consensus in blockchain sharding[J]. ACM Transactions on Internet Technology, 2023, 23(2): 1-27.

[53] LIU Y Z, XIA Y, LIU J W, et al. A secure and decentralized reconfiguration protocol for sharding blockchains[C]// 2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security. Piscataway: IEEE, 2021: 111-116.

[54] GADIRAJU D S, LALITHA V, AGGARWAL V. Secure regenerating codes for reducing storage and bootstrap costs in sharded blockchains[C]//2020 IEEE International Conference on Blockchain. Piscataway: IEEE, 2020: 229-236.

[55] HONG Z C, GUO S, LI P, et al. Pyramid: A layered sharding blockchain system[C]//IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. New York: ACM, 2021: 1-10.

[56] ZHANG M Q, LI J C, CHEN Z H, et al. CycLedger: A scalable and secure parallel protocol for distributed ledger via sharding[C]//2020 IEEE International Parallel and Distributed Processing Symposium. Piscataway: IEEE, 2020: 358-367.

[57] EOS. team IO. EOS. IO technical white paper v2[R/OL]. (2017-06-26) [2025-05-02]. https://github. com/EOSIO/Documentation.

[58] XU G X, LIU Y, KHAN P W. Improvement of the DPoS consensus mechanism in blockchain based on vague sets[J]. IEEE Transactions on Industrial Informatics, 2020, 16(6): 4252-4259.

[59] LUO Y H, CHEN Y Q, CHEN Q, et al. A new election algorithm for DPos consensus mechanism in blockchain[C]// 2018 7th International Conference on Digital Home. Piscataway: IEEE, 2018: 116-120.

[60] ABRAHAM I, NAYAK K, REN L, et al. Brief note: Fast authenticated byzantine consensus[EB/OL]. (2022-04-29)[2025-05-02]. https://arxiv.org/pdf/2102.07932.

[61] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]//Proceedings of the Third Symposium on Operating Systems Design and Implementation. New York: ACM, 1999: 173-186.

[62] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: A distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference. New York: ACM, 2018: 1-15.

[63] SHAHRIAR HAZARI S, MAHMOUD Q H. Improving transaction speed and scalability of blockchain systems via parallel proof of work[J]. Future Internet, 2020, 12(8): 125.

[64] RAZA Z, HAQ I U, MUNEEB M, et al. Energy efficient multiprocessing solo mining algorithms for public blockchain systems[J]. Scientific Programming, 2021, 2021: 9996132.

[65] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-ng: A scalable blockchain protocol[C]//13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16). Berkeley: USENIX, 2016: 45-59.

[66] VASIN P. Blackcoin's proof-of-stake protocol v2[EB/OL]. (2014-02-28) [2025-05-02]. https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper.pdf.

[67] BUTERIN V, GRIFFITH V. Casper the friendly finality gadget[EB/OL]. (2017-10-25) [2025-05-02]. https://arxiv. org/pdf/1710.09437.pdf.

[68] SKH SAAD S M, RAJA MOHD RADZI R Z. Comparative review of the blockchain consensus algorithm between proof of stake (POS) and delegated proof of stake (DPOS)[J]. International Journal of Innovative Computing, 2020, 10(2): 27-32.

[69] 靳世雄, 张潇丹, 葛敬国, 等. 区块链共识算法研究综述[J]. 信息安全学报, 2021, 6(2): 85-100.
JIN S X, ZHANG X D, GE J G, et al. Overview of blockchain consensus algorithm[J]. Journal of Cyber Security, 2021, 6(2): 85-100. (in Chinese)

[70] RIEHL J R, WARD J. Transaction pricing for maximizing throughput in a sharded blockchain ledger[C]//2020 Crypto Valley Conference on Blockchain Technology. Piscataway: IEEE, 2020: 36-42.

[71] KHAN S N, LOUKIL F, GHEDIRA-GUEGAN C, et al. Blockchain smart contracts: Applications, challenges, and future trends[J]. Peer-to-Peer Networking and Applications, 2021, 14(5): 2901-2925.

[72] GAO Z M, XU L, CHEN L, et al. Scalable blockchain based smart contract execution[C]//2017 IEEE 23rd International Conference on Parallel and Distributed Systems. Piscataway: IEEE, 2017: 352-359.

[73] SOLIDITY Team. Solidity Docs[EB/OL]. (2016-02-28)[2025-05-02]. https://docs.soliditylang.org/en/latest/.

[74] POON J, DRYJA T. The bitcoin lightning network: Scalable off-chain instant payments[EB/OL]. (2016-01-14) [2025-05-02]. https://1bitcoin.ca/s/lightning-network-paper.pdf.

[75] Raiden Network Website. Fast, cheap, scalable token transfers for Ethereum[EB/OL]. (2023-02-28) [2025-05-02]. https://raiden.network/.

[76] DECKER C, WATTENHOFER R. A fast and scalable payment network with Bitcoin duplex micropayment channels[C]//Stabilization, Safety, and Security of Distributed Systems. Cham: Springer, 2015: 3-18.

[77] MILLER A, BENTOV I, BAKSHI S, et al. Sprites and state channels: Payment networks that go faster than lightning[C]//Financial Cryptography and Data Security. Cham: Springer, 2019: 508-526.

[78] KHALIL R, GERVAIS A. Revive: Rebalancing off-blockchain payment networks[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 439-453.

[79] ROHRER E, LAß J F, TSCHORSCH F. Towards a concurrent and distributed route selection for payment channel networks[M]//Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham: Springer International Publishing, 2017: 411-419.

[80] SIVARAMAN V, VENKATAKRISHNAN S B, RUAN K, et al. High throughput cryptocurrency routing in payment channel networks[C]//17th {USENIX} Symposium on Networked Systems Design and Implementation. Berkeley: USENIX, 2020: 777-796.

[81] Loom network community. Loom network documentation [EB/OL]. (2023-02-28)[2025-05-02]. https://loomx.io.

[82] LERNER S D. RSK: Bitcoin powered smart contracts[EB/OL]. (2022-02-28) [2025-05-02]. https://rootstock. io/rsk-white-paper-updated.pdf.

[83] POON J, BUTERIN V. Plasma: Scalable autonomous smart contracts[EB/OL]. (2017-08-11) [2025-05-02]. https://plasma.io/plasma-deprecated.pdf.

[84] Foundation fusion. Fushion: An inclusive cryptofinance platform based on blockchain[EB/OL]. (2023-02-28) [2025-05-02]. https://www. fusion. org/themes/fusion/assets/pdf/Fusion-White-Paper.pdf.

[85] KWON J, BUCHMAN E. Cosmos: A network of distributed ledgers[EB/OL]. (2018-02-28) [2025-05-02]. https://v1.cosmos.network/cosmos-whitepaper.pdf.

[86] TEUTSCH J, REITWIEßNER C. A scalable verification solution for blockchains[EB/OL]. (2023-02-28) [2025-05-02]. https://arxiv.org/pdf/1908.04756.

[87] BODORIK P, LIU C G, JULTA D. Using FSMs to find patterns for off-chain computing: Finding patterns for off-chain computing with FSMs[C]//Proceedings of the 2021 3rd International Conference on Blockchain Technology. New York: ACM, 2021: 28-34.

[88] FREY D, MAKKES M X, ROMAN P L, et al. Bringing secure Bitcoin transactions to your smartphone[C]//Proceedings of the 15th International Workshop on Adaptive and Reflective Middleware. New York: ACM, 2016: 1-6.

[89] ZHENG Q H, LI Y, CHEN P, et al. An innovative IPFS-based storage model for blockchain[C]//2018 IEEE/WIC/ACM International Conference on Web Intelligence. Piscataway: IEEE, 2018: 704-708.

[90] DOAN T V, BAJPAI V, PSARAS Y, et al. Towards decentralised cloud storage with IPFS: Opportunities, chal-

lenges, and future directions[EB/OL]. (2022-01-01)[2025-05-02]. https://arxiv.org/pdf/2202.06315.

[91] HE G B, SU W, GAO S. Chameleon: A scalable and adaptive permissioned blockchain architecture[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking. Piscataway: IEEE, 2018: 87-93.

[92] LI C L, HUANG H W, ZHAO Y T, et al. Achieving scalability and load balance across blockchain shards for state sharding[C]//2022 41st International Symposium on Reliable Distributed Systems. Piscataway: IEEE, 2022: 284-294.

[93] LIU Y Z, LIU J W, SALLES M A V, et al. Building blocks of sharding blockchain systems: Concepts, approaches, and open problems[J]. Computer Science Review, 2022, 46: 100513.

[94] WANG G, SHI Z J, NIXON M, et al. SoK: Sharding on blockchain[C]//Proceedings of the 1st ACM Conference on Advances in Financial Technologies. New York: ACM, 2019: 41-61.

[95] JIA L P, LIU Y X, WANG K Y, et al. Estuary: A low cross-shard blockchain sharding protocol based on state splitting[J]. IEEE Transactions on Parallel and Distributed Systems, 2024, 35(3): 405-420.

[96] LI M Z, LIN Y, ZHANG J, et al. CoChain: High concurrency blockchain sharding via consensus on consensus[C]// IEEE INFOCOM 2023 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2023: 1-10.

[97] LI M Z, WANG W, ZHANG J. LB-chain: Load-balanced and low-latency blockchain sharding via account migration[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(10): 2797-2810.

[98] KRÓL M, ASCIGIL O, RENE S, et al. Shard scheduler: Object placement and migration in sharded account-based blockchains[C]//Proceedings of the 3rd ACM Conference on Advances in Financial Technologies. New York: ACM, 2021: 43-56.

[99] ZHANG Y Z, PAN S R, YU J S. TxAllo: Dynamic transaction allocation in sharded blockchain systems[C]//2023 IEEE 39th International Conference on Data Engineering. Piscataway: IEEE, 2023: 721-733.

[100] HUANG X, JIE W, ZHANG S, et al. ContribChain: A stress-balanced blockchain sharding protocol with node contribution awareness[C]//IEEE INFOCOM 2025 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2025: 1-10.

[101] HONG Z, GUO S, ZHOU E, et al. Gridb: Scaling blockchain database via sharding and off-chain cross-shard mechanism[EB/OL]. (2024-07-04)[2025-05-02]. https://arxiv.org/abs/2407.03750.

[102] PARK S, MUN B, LEE S, et al. Impact of eip-4844 on ethereum: Consensus security, ethereum usage, rollup transaction dynamics, and blob gas fee markets[EB/OL]. (2024-03-06)[2025-05-02]. https://arxiv.org/abs/2405.03183.

[103] XIE J, ZHANG K, LU Y L, et al. Resource-efficient DAG blockchain with sharding for 6G networks[J]. IEEE Network, 2022, 36(1): 189-196.

[104] ROHRER E, TSCHORSCH F. Kadcast-NG: A structured broadcast protocol for blockchain networks[J]. IEEE/ACM Transactions on Networking, 2023, 31(6): 3269-3283.

[105] HELLINGS J, SADOGHI M. ByShard: Sharding in a Byzantine environment[J]. The VLDB Journal, 2023, 32(6): 1343-1367.

[106] TAO Y C, LI B, LI B C. On sharding across heterogeneous blockchains[C]//2023 IEEE 39th International Conference on Data Engineering. Piscataway: IEEE, 2023: 477-489.

[107] HONG Z C, GUO S, ZHOU E Y, et al. Prophet: Conflict-free sharding blockchain via Byzantine-tolerant deterministic ordering[C]//IEEE INFOCOM 2023 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2023: 1-10.

[108] XU J, MING Y L, WU Z H, et al. X-shard: Optimistic cross-shard transaction processing for sharding-based blockchains[J]. IEEE Transactions on Parallel and Distributed Systems, 2024, 35(4): 548-559.

[109] LIU A D, LIU Y Z, WU Q H, et al. CHERUBIM: A secure and highly parallel cross-shard consensus using quadruple pipelined two-phase commit for sharding blockchains[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 3178-3193.

[110] CHEN Q D, HUANG H W, YIN Z K, et al. Broker2Earn: Towards maximizing broker revenue and system liquidity for sharded blockchains[C]//IEEE INFOCOM 2024 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2024: 251-260.

[111] Team Avail. Avail: A unifying blockchain network: Version: 2.1[EB/OL]. (2024-11-06)[2025-05-02]. https://github.com/availproject/data-availability/blob/93c547ce4efce3e992b573179a8d22b3657fdcee/reference%20document/Avail%20Reference%20Paper%20v2.1%206%20Nov%202024.pdf.

[112] QI X D. S-store: A scalable data store towards permis-

sioned blockchain sharding[C]//IEEE INFOCOM 2022 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2022: 1978-1987.

[113] HUANG H W, ZHAO Y T, ZHENG Z B. tMPT: Reconfiguration across blockchain shards via trimmed merkle patricia trie[C]//2023 IEEE/ACM 31st International Symposium on Quality of Service. Piscataway: IEEE, 2023: 1-10.

[114] CAI Z T, LIANG J Y, CHEN W H, et al. Benzene: Scaling blockchain with cooperation-based sharding[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(2): 639-654.

[115] HUANG H W, YUE Z Y, PENG X W, et al. Elastic resource allocation against imbalanced transaction assignments in sharding-based permissioned blockchains[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 33(10): 2372-2385.

[116] JIANG S, CAO J N, TUNG C L, et al. Sharon: Secure and efficient cross-shard transaction processing via shard rotation[C]//IEEE INFOCOM 2024 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2024: 2418-2427.

[117] ZHANG J T, CHEN W H, HONG Z C, et al. Efficient execution of arbitrarily complex cross-shard contracts for blockchain sharding[J]. IEEE Transactions on Computers, 2024, 73(5): 1190-1205.

[118] HUANG H W, LIN Y, ZHENG Z B. Account migration across blockchain shards using fine-tuned lock mechanism[C]// IEEE INFOCOM 2024 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2024: 271-280.

[119] ZHANG C, XU C, HU H, et al. {COLE}: A column-based learned storage for blockchain systems[C]//22nd USENIX Conference on File and Storage Technologies (FAST 24). Berkeley: USENIX, 2024: 329-345.

[120] HUANG H W, YE G, YANG Q L, et al. BlockEmulator: An emulator enabling to test blockchain sharding protocols[J]. IEEE Transactions on Services Computing, 2025, 18(2): 690-703.

作者简介

蒋凌云 女,1978年4月出生于湖南省永州市. 现为南京邮电大学副教授、硕士生导师. 主要研究方向为区块链、信息网络与智能信息处理.
E-mail: jianglingyun@njupt.edu.cn

叶 飞 男,1998年12月出生于江苏省宿迁市. 主要研究方向为区块链.
E-mail: 1006537138@qq.com

杨京霖 男,2001年9月出生于山东省临沂市. 现为南京邮电大学硕士. 主要研究方向为区块链.
E-mail: 15106603428@163.com

徐 佳 男,1980年10月出生于江苏省常州市. 现为南京邮电大学教授,博士生导师. 主要研究方向为无线充电网络、智能信息处理. 中国电子学会会员编号:E190011107M.
E-mail: xujia@njupt.edu.cn

马鹏程 男,2002年1月出生于江苏省泰州市. 现为南京邮电大学硕士. 主要研究方向为区块链.
E-mail: 1500217687@qq.com

刘婷婷 女,1982年10月出生于江苏省淮安市. 现为南京邮电大学教授、硕士生导师. 主要研究方向为多模态机器学习、近似理论、博弈论、优化理论、排队理论、网络资源管理等.
E-mail: liutt@njupt.edu.cn