计算机科学
COMPUTER SCIENCE

区块链分片技术研究综述

谭朋柳，徐滕，涂若欣

引用本文

谭朋柳，徐滕，涂若欣. 区块链分片技术研究综述[J]. 计算机科学，2024，51(11)：307-320.

TAN Pengliu, XU Teng, TU Ruoxin. Review of Research on Blockchain Sharding Techniques[J]. Computer Science, 2024, 51(11): 307-320.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231200078

区块链分片技术研究综述

谭朋柳　徐　滕　涂若欣
南昌航空大学软件学院　南昌 330063

摘　要　区块链技术以去中心化、防篡改等功能为特色，具有广泛的应用前景。然而，区块链系统难以支撑大规模海量的分布式数据管理和交易，所以区块链的性能和可扩展性问题成为重要的研究方向。目前，研究人员分别从修改链上的数据结构和共识算法，到添加链下操作技术，提出了一些解决方案，以提高区块链的性能和可扩展性。而其中，随着网络规模的增加，实现水平扩展性的最实用的方法就是分片技术。作为一种链上扩容方式，分片技术是一种将整个区块链网络划分成多个片段的方法，便于同时处理多个交易或合约。每个分片都可以独立运行，拥有自己的交易历史和状态，在不牺牲中心化程度的同时提高了区块链的性能和可扩展性。以往的大量区块链分片技术研究着重介绍了分片中的交易共识，而忽略了分片策略机制与分片架构。为此，首先对现有的分片区块链进行系统分析，将分片区块链的设计过程分为架构设置、节点选择、节点分配、交易分发、交易处理和分片重构等部分，并分析了分片区块链的设计过程的各部分的功能、属性；其次，对分片架构进行了分类和总结，重点研究了各种分片策略与机制，分析了它们的优缺点；之后，对主流的分片区块链系统做了比较，并分析了它们的可扩展性和可靠性，包括系统吞吐量、时延、通信开销、节点随机性、分片安全性和跨片智能合约等；最后，提出未来可能的研究方向。

关键词：区块链；分布式账本技术；可扩展性；分片技术；并行处理
中图分类号　TP301

Review of Research on Blockchain Sharding Techniques

TAN Pengliu，XU Teng and TU Ruoxin
School of Software，Nanchang Hangkong University，Nanchang 330063，China

Abstract　Blockchain technology is characterized by decentralization and tamper resistance，and has a wide range of application prospects. However，it is difficult for blockchain systems to support large-scale distributed data management and transactions，so the performance and scalability of blockchain have become important research directions. At present，researchers have proposed some solutions to improve the performance and scalability of blockchain by modifying the data structure and consensus algorithm on the chain，and adding off-chain operation technology. Among them，the most practical method to achieve horizontal scalability with the increase of network scale is sharding technology. As an on-chain scaling method，sharding technology is a method to divide the entire blockchain network into multiple segments to facilitate the simultaneous processing of multiple transactions or contracts. Each shard can operate independently，with its own transaction history and state，improving the performance and scalability of the blockchain without sacrificing centralization. Previous studies on blockchain sharding technology have focused on introducing transaction consensus in sharding，while ignoring the sharding strategy mechanism and sharding architecture. Therefore，this paper first systematically analyzes the existing sharding blockchains，divides the design process of sharding blockchains into several parts：architecture setting，node selection，node allocation，transaction distribution，transaction processing，and sharding reconstruction，and analyzes the functions and properties of each part of the design process of sharding blockchains. Secondly，the sharding architecture is classified and summarized. This paper focuses on various sharding strategies and mechanisms，analyzes their advantages and disadvantages，compares mainstream sharding blockchain systems，and analyzes their scalability and reliability，including system throughput，delay，communication overhead，node randomness，sharding security，and cross-shard smart contracts. Finally，future research directions are proposed.

Keywords　Blockchain，Distributed ledger technology，Scalability，Sharding technology，Parallel processing

---

到稿日期：2023-12-12　返修日期：2024-05-09
基金项目：国家自然科学基金(61961029)；江西省科技厅重点研发计划(20171ACE50025)
This work was supported by the National Natural Science Foundation of China(61961029) and Key Research Plan of Science and Technology Department of Jiangxi Province(20171ACE50025).
通信作者：谭朋柳(pltan@nchu.edu.cn)

1 引言

分片思想[1]最初是由传统的集中式数据库领域引入的，它将整个数据库划分为单独的部分，称为分片。在区块链系统中，分片指将分布式账本系统中的节点按照一定机制划分为若干集合。通常，一个集合被称为一个委员会。系统以委员会为单位来对交易进行处理。各个委员可以并行验证及执行与其不相交的交易集对应的交易，必要时进行跨片通信，保证系统统一的全局状态，共同维护账本数据结构。在传统的区块链网络中，每个节点负责处理所有交易，而分片中的节点只维护区块链数据分类账的一部分，无须处理与存储全部的交易数据，整个区块链的处理能力也不会受限于全网中的某一节点的计算能力，实现网络处理能力的可扩展性，从而提高了区块链流程的效率。在区块链应用快速发展的推动下，基于区块链的分片技术因迫切的实际需求而得到广泛研究。

迄今为止，已有许多关于区块链分片系统的相关研究问世，每项研究都有不同的侧重点。文献[2]概述了最先进的分片方案，将区块链分片技术的结构分解为 4 个功能相交的基础层，包括数据层、成员层、分片内层和跨分片层，并分析了 4 种代表性的分片方案（ELASTICO[3]，OmniLedger[4]，RapidChain[5]和 Monoxide）的吞吐量理论上限。文献[6]提出了一个全面的框架来分析分片方案的安全性和性能，将区块系统进行分片的整个过程分为 7 个阶段，但缺乏适当的分类和对分片方案的全面审查。文献[7]对各种分片方案进行了简要总结，简单描述了将分片过程分为常见的关键组件，重点强调了各个组件会受到何种攻击，并提出了相应对策，但是缺乏对各个组件深入的分析和比较。文献[8]主要关注分片区块链系统中，随着参与节点数量的不断增加，系统性能方面的挑战。综上，已有工作缺乏适当的分类和对分片方案的全面研究。

本文对现有主流区块链分片技术进行分析研究。首先，分片区块链系统结构复杂，它们通常包含若干个关键模块，如分片架构的设置、分片内成员的确定、节点分片、交易处理、节点重分片配置等。但目前各个模块的功能研究不够清晰，这导致难以探索每个模块的升级替代设计。其次，没有足够明确地评估现有区块链分片系统，探索系统模块化设计的架构。共识机制[9]在交易处理时对区块链系统非常关键，在很大程度上决定了系统的安全性和性能。如，一些共识机制可能更容易受到攻击或操纵，从而影响分片的安全性；不同的共识机制可能需要不同的计算和通信开销来完成分片网络中的共识过程，影响共识时延；共识机制应该能够在分片网络中有效地进行交易确认和区块验证，同时克服分片之间的通信和同步问题，以实现整个系统的高度可扩展性。但由于区块链共识机制[10]的相关研究已经相当充分，也有许多文章专门介绍区块链分片共识，因此本文不再另外研究该内容。

2 相关理论

2.1 分片的 3 种类型

区块链分片技术通常包括网络分片、交易分片和状态分片。3 种技术的融合可以提高区块链系统的性能和扩展性。

其中，网络分片是最基本的分片方案，是交易分片与状态分片的基础。网络分片将整个区块链网络分成多个子网络，每个子网络只处理一部分交易和区块。交易分片是在网络分片之后，将未确认的交易按照相应的规则分配到各个分片中进行处理，每个分片可以并行地处理交易，从而提高区块链交易的处理能力，加快交易确认速度，并且有效地减轻整个网络的负载压力。状态分片将区块链网络的全局状态拆分为不同的分片。与交易分片不同，状态分片中的每个节点仅存储整个区块链系统数据的一部分，这显著降低了存储负担，但需要额外的备份来维护区块链的完整全局状态，以防止分片内的损坏。3 种分片技术的关系如图 1 所示。

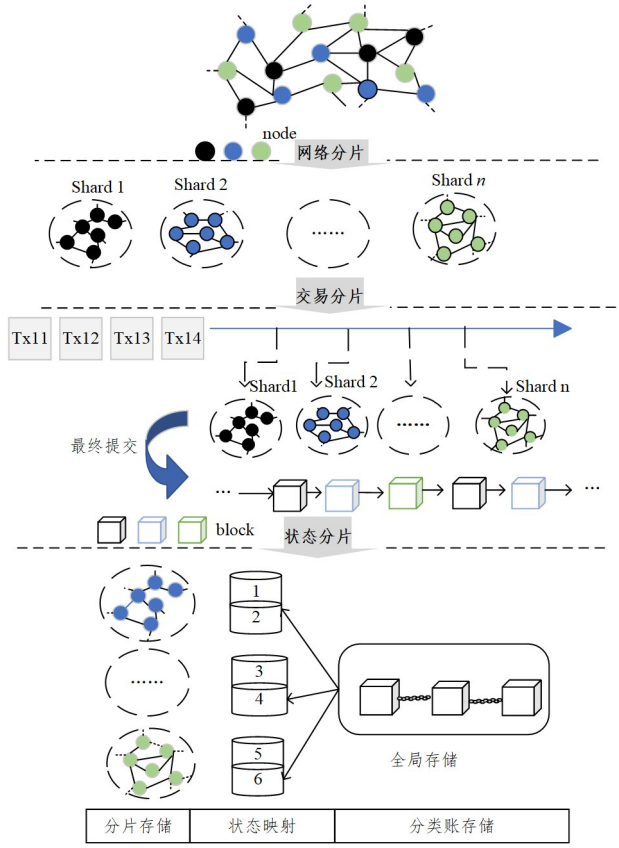

图 1 3 种技术的关系

Fig. 1 Relationship among three technologies

2.2 区块链的分片步骤

在区块链分片技术中，节点首先需要建立身份验证，在分片建立和设置阶段，节点和交易被随机划分到不同的分片中。分片内的节点可以自由地共享它们的身份并彼此建立连接。之后，同一个分片中的节点进行分片内共识以商定一组交易，而不同分片之间的节点执行跨分片共识以实现全局状态。最后，为了维护系统安全性，分片系统周期性地将节点重新分配到不同的分片中。

区块链分片通常涉及 6 个主要流程部分，如架构设置、节点选择、节点分配、交易分发、交易处理和分片重新配置。每个部分可以通过不同的方法实现，然后将所有模块组合在一起，从而获得完整的分片区块链系统。图 2 为分片系统概要流程图。

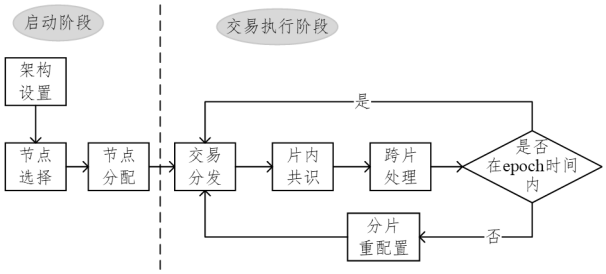

图 2　分片流程图

Fig. 2　Sharding flowchat

1)架构设置：在分片系统初始设置阶段，根据需求选择有主链作为中转的星型架构或分片间直接交互的无主链平行架构。

2)节点选择：许可区块链通过可信第三方验证节点选择节点，非许可区块链通过共识机制选择节点，从而防御女巫攻击。每个节点需要建立身份认证，即由公钥、IP 地址和工作量证明解决方案组成的身份认证。

3)节点分配：在协议的开始阶段对节点进行分片的过程中，分片函数的设计往往以节点身份(IP 地址、PK、Hash)、节点标识中的一些字节、自身分片位置或节点的地址作为输入变量，各个节点划分到分片后，同一分片节点之间进行广播，最终完成分片内节点信息的交流。其中，每个参与区块链网络的节点都拥有一个唯一的 IP 地址；PK 是每个节点通常都有的公钥(Public Key)，一般用于加密和验签消息；节点的身份信息经过哈希函数处理后得到的结果就是其哈希值(Hash)。IP 地址、PK 和 Hash 均可以用来唯一地标识一个节点。每次节点的分配结果会持续一个固定时间，即一个 epoch。

4)交易分发：系统按照交易到各个分片的映射规则来分发交易。

5)交易处理。

(1)片内共识：对于片内交易，委员会内部对交易形成片内共识。

(2)跨片处理：对于跨分片的交易，交易应该在整个系统中原子地提交。跨片交易的处理可以分为两个阶段。在第一阶段，输入分片生成证明来证明交易输入是否可用，并将证明发送到相关分片；在第二阶段，所有相关分片通过收到的证明来验证交易是否有效。

如图 3 所示，同一个分片中的节点大部分时间只需要执行分片内的通信，并将一些关键信息发送给分片的委员会节点，委员会节点通常负责跨分片通信以及分片内共识，每个分片至少有一个委员会节点。一般来说，委员会节点需要具有比其他分片内节点更强的通信能力。

6)分片重构：为了保证分片的安全性，避免恶意节点涌入某一分片，且减少跨分片交易，需要每隔 epoch 时间对所有分片进行重新配置，这也要求重新配置需要具有一定的随机性。

如图 4 所示，参与节点代表所有希望参与协议的节点，合格节点表示选定的新节点，分片 1 代表已确定的委员会。从参与节点到合格节点的身份转变，需要有像 PoW 这样的机制来防御女巫攻击。在节点配置环节，需要一个安全的随机性来将选定的节点分配到多个委员会中。

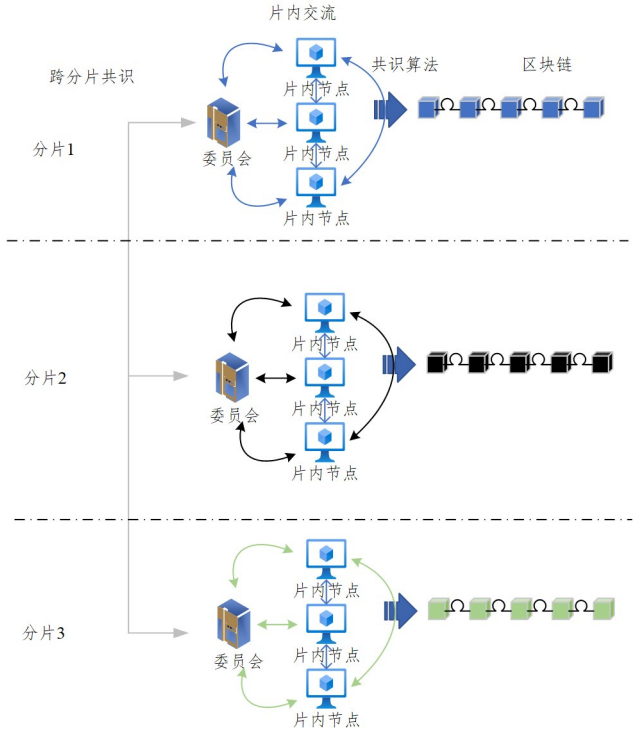

图 3　分片区块链系统中的通信

Fig. 3　Communication in a sliced blockchain system

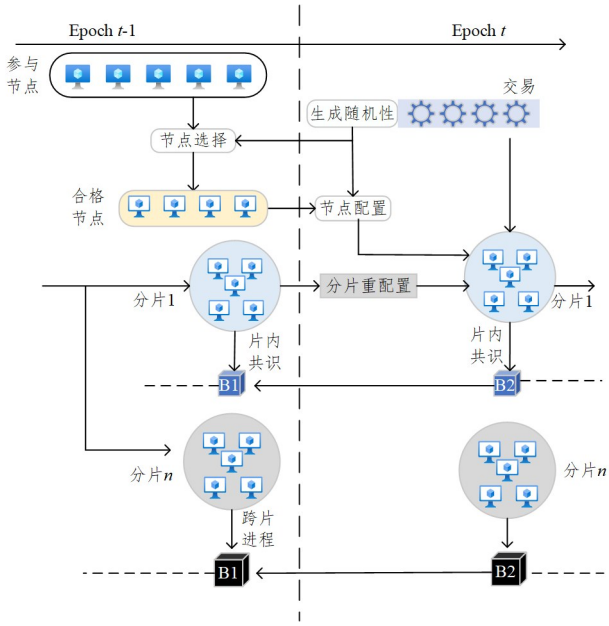

图 4　分片中各部分之间的关系

Fig. 4　Relationship between parts in sharding

2.3　Epoch 随机性

随机性用于在开始阶段和每个重新配置阶段，将节点分配到不同的分片，选择每个分片的领导节点或委员会节点，决定跨分片事务应当广播到哪些分片等。Epoch 随机性是每个诚实节点通过与参与者的交互获得相同的随机性，在区块链分片技术中有助于增加分布式网络的公平性和安全性，降低集中化风险，并提高整体系统的可用性。下面介绍 Epoch

随机性在区块链分片技术中的具体作用。

1)共识随机性:Epoch 随机性可以用于选择哪个验证节点(或验证组)负责生成区块或执行共识算法。这个选择可以通过随机选取某个节点或组,或者通过轮换不同的节点或组来完成。这种随机性有助于分布式网络中公平地分配任务,防止某些节点集中化控制整个网络,同时提高安全性。

2)验证节点轮换:Epoch 随机性可以用于确定哪些验证节点将负责验证交易和创建区块。可以定期更换验证节点的身份,以确保没有特定节点获得过多的权力,防止潜在的不当行为。

3)数据随机性:在某些区块链分片技术中,数据可能会被分片并存储在不同的节点上。Epoch 随机性可以用于确定数据的分布方式,以确保数据均匀地存储在不同的节点上,降低数据的单点故障风险。

4)防御攻击:Epoch 随机性可以增加区块链分片网络的安全性。通过在共识和验证过程中引入随机性,攻击者难以预测哪些节点或分片会被攻击,从而增加了攻击的难度。

3 分片架构

近年来,区块链系统的分片方案研究按照并行化架构可分为两种:有主链作中转的星型架构和无主链的分片间直接交互的平行架构[11]。不同的架构性能并非针对网络分片、交易分片、状态分片中的某一种类型,而是为了涵盖采用架构分片的普遍情况。

如图 5 所示,平行架构是将原有的区块链系统拆分为多条子链(分片),每个节点仅维护特定分片,并验证该分片内部的交易。通过这种方式,每笔交易仅由一部分节点处理,各分片间实现了交易处理的并行化,进而实现了区块链系统效能的提升。星型架构将分片链都锚定在主链之上,分片链借助主链进行更高层次的共识,主链约束并管理分片链,跨分片交易要么拆分为分片内的交易,要么由主链同时协助分片链完成跨分片通信。

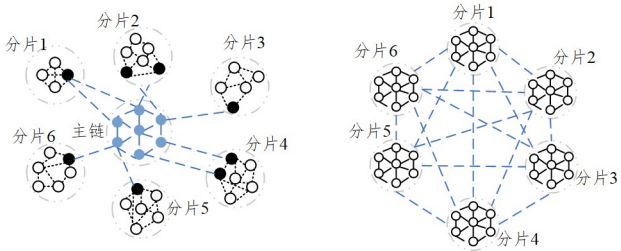

图 5 通用区块链的架构模型

Fig. 5 Architectural model of generic blockchain

3.1 平行架构

平行架构是一种无需主链的架构,整个区块链的账本被分成若干份互不相交的账本并存储在分片节点中,各个分片维护自己的账本,整个区块链网络的各个分片合起来拥有完整的账本。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,由某一分片内的节点保障跨片交易的原子性和分片间的一致性。

Monoxide,Chainspace[12] 和 Ostraka[13] 均通过用平行架构设计分片区块链系统,考虑到每个节点处理事务的能力不同,采用节点差异环境模型。但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。Benzene[14] 建立了功能解耦的双链架构,该架构将交易记录功能与共识执行功能分离,从而在保持分片并发性的同时,实现共识执行过程中的跨分片协作,提高了容错性。

3.2 星型架构

星型架构是一种主链-分片链架构,其中主链负责交易的最终确认并为系统提供安全保障,分片链需维护自身分片并同步主链与本分片的数据。根据主链功能的不同,分为两种情况。第一种情况是主链只处理跨片交易,但不存储整个网络的状态数据,即分片达成共识后采用交易集中方法,分片间指定新的交易地址,将所有跨片交易统一处理,由主链进行处理转发;第二种情况是主链节点存储完整的分类账,分片链在最终共识过程中,每个分片网络会生产区块并验证储存于区块内的数据,将处理完的区块传输到主链,主链接受各分片网络的区块,同时负责数据的最终验证,最后将各个区块排序上链存储,完成整个过程。

Ethereum 2.0[15] 分片项目是将整个区块链进行分片,将区块链划分为现有的以太坊主链和分片链,同时设计了信标链负责连接主链和对分片的管理,跨分片交易需要信标链为中介进行验证。当系统中跨分片交易数量过多时,单一的主链或者委员会却可能因为无法负载大量交易的转发工作而阻塞甚至崩溃,成为区块链系统的性能瓶颈。Polkadot[16] 网络中采用的是中继链-平行链架构,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,基础的业务可以仅在平行链内执行完成,只有部分交易涉及中继链的资产或需要与其他平行链交互。因此,Polkadot 要求片内交易占据较大的交易比例。Ethereum 2.0 和 Polkadot 都致力于做到状态分片,它们均是由分片维护片内的状态,每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复杂度较高,主链处理交易的速度较慢。

SSchain[17] 同样也采用双层网络结构。第一层是根区块链网络,这种结构类似于原始的比特币网络,其中节点存储完整的分类账,可以在交易提交前验证每个分片的块。第二层是分片网络,由多个分片组成,每个分片内的事务由 POW 共识处理。根区块链对分片生成的区块进行第二次验证,以防止双重花费攻击。在 SSchain 中,鼓励用户尽可能多地使用分片内交易,以获得更快的交易确认和更低的费用。图 6 所示为 SSchain 跨分片交易方法,如果一笔交易有多个输入地址,用户的钱包会自动将其拆分为多个分片内交易。其余无法拆分的跨分片交易被转发到根链,根链保存完整的账本,可以直接验证跨分片交易。根链在整个网络中占据了很大一部分哈希算力,以维护系统安全。由于分片块是由根链网络验证的,恶意对手至少需要根链一半的算力才能进行双花攻击。

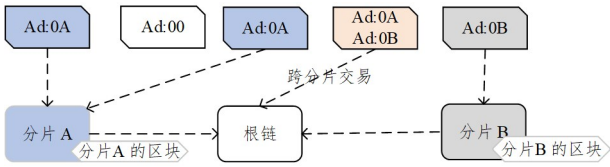

图 6 SSchain 跨分片交易方法

Fig. 6 SSchain cross-split transaction method

基于 POW 和 BFT 混合共识协议的 Omniledger[4] 分片架构，由一个身份链以及多个分片子链构成，实现系统吞吐量与分片数量的线性增加，使用星型架构的通信与存储开销相对减少。文献[18]介绍了一个用于中药溯源的分片区块链系统，该系统架构由一个领导者分片区块链层作为其主要组件，采用分片机制来方便中医药追踪。当分片中确定提交某个区块后，会更新本分片状态与总系统状态。系统中存在一条总链，用于整合各个分区的子链信息，分片内节点只需要存储当前分片的区块链数据，使分区型区块链在物理上多链而逻辑上单链。Sun 等[19] 使用虚拟化技术将分片区块链设置为一条主链和 M 条分片链，主链负责管理整个分片系统，即将 N 个物理节点转化为 N 个虚拟节点，通过随机算法对虚拟节点进行身份标识，进而根据虚拟化身份将 N 个物理节点分配到 M 个分片上并进行进一步的资源优化。Wang 等[11] 通过研究主链性能与分片数量关系得出星型分片架构的通用模型，旨在分析其性能边界与性能瓶颈，以平衡分片数量和主链功能的复杂度。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。减少处理跨片交易产生的通信开销等问题，是提升星型分片性能的关键。

4 分片策略

每个分片对应一个委员会，其负责处理片内交易。系统中多个委员会可以并行处理交易，提升账本系统的吞吐量。通过将节点划分至各委员，并将交易分发至各委员会，各委员会并发处理交易，系统的并发度得到提升。委员会的产生机制，即节点分片机制，是性能优化的一个关键环节。图 7 给出了节点选择和节点分配过程。本章将分片机制分为基于节点属性的分片机制与基于交易的分片机制。

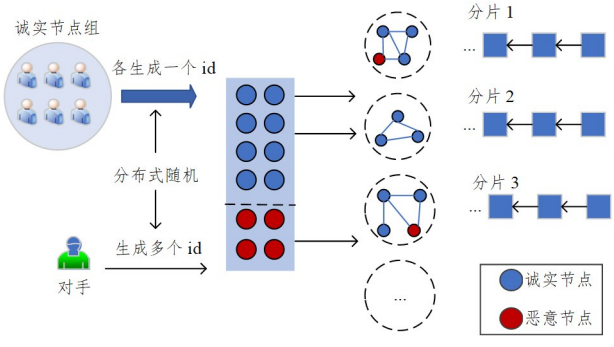

图 7 节点选择和节点分配过程

Fig. 7 Node selection and node allocation process

4.1 基于节点属性的分片策略

基于节点分片是减少通信开销和实现并行交易事务处理的关键。通常情况下，节点分配应该禁止节点自由选择加入哪个分片，以防止恶意节点聚集在一个分片中。此外，每个分片中的节点数量应该平衡，以便每个分片能够高效地处理交易。节点分片通常应遵循 3 个属性，如表 1 所列。

表 1 基于节点分片的 3 个属性

Table 1 Three attributes based on node slicing

属性	说明
公共可验证性	一旦使用新的分片策略，所有各方都可以仅使用公共信息验证
有效性	诚实节点必须及时分配到分片中
无偏性	节点分配过程不受外部干扰，且任何单个参与者或共谋对手都不能阻止进程
随机性	参与节点被随机分配到不同的分片

将节点分配方法分为静态优化方法和动态优化方法。静态分配优化方法基于节点的身份或通过采用随机生成器将节点分配给分片；动态分配优化方法采用深度强化学习、机器学习算法等提供增强分片系统的安全性和自适应性的多功能方法；节点属性根据一段时间内累积的交易内容对片间状态的分布重新调整。该过程兼顾状态调整后每个分片处理的交易量和跨分片交易比例，同时通过“账户分割”机制来进一步缓解热分片负载和减少跨片交易。

4.1.1 节点分片的静态优化方法

目前，基于节点分片的主要静态优化方法有以下 3 种。

1）基于 hash 算法的分片机制。节点形成各自的 hash 串，系统截取 hash 串中固定位置的 s 位 hash bit 进行运算，将其映射到2^n个分片中。表 2 对基于 hash 算法的 4 种分片机制进行介绍。

与上述哈希算法不同的是，Elastico[3] 中将节点的身份信息（IP 地址/PK 公钥）和对应的委员会信息结合 epochRandomness 函数来建立身份并组建委员会。由 epochRandomness 函数计算出满足式（1）条件的 nonce，根据 nonce 值确定分片位置，随后进行广播。

$$O=H(epochRandomness||IP||PK|nonce)\leqslant 2^{r-D} \quad (1)$$

其中，D 为预定义的工作量证明难度，r 为预定义的 H 函数的输出位数，最后计算得到的这个哈希值 O 也会被作为节点的 ID，每个节点根据自己的 O 值确定分片位置。在 Elastico 系统中，会创建2^s个委员会，每个委员会拥有一个 s 位的 ID。协议会根据 s 位的 ID 来随机地分配节点。但目前没有任何机制可以审计 Elastico 当前的分片委员会节点的数量，且其要求离线调整委员会的数量 s，限制了分片数量的动态性，故障概率高。

2）基于随机分片机制。随机分配节点主要针对分片构成中可能存在的恶意节点不均匀分布，即恶意节点聚合在某个分片内造成的系统安全问题。总体思路是通过随机函数使每个节点都获得相同的随机数，每个节点都可以使用该随机数作为种子来获得元素为[1∶N]的一个随机全排列 π。因为种子是一样的，所以每个节点的随机全排列 π 也是一样的，再将 π 划分为 k 份，每一份便是一个分片委员会，这样可以使恶意节点均匀地分配到各个分片中。随机数生成器是一种具有无偏向分布式随机性的可公开验证的安全多方计算协议，可使各节点具有既安全又不可控的身份标识。下面介绍几种随机数生成器。

表 2 基于 hash 算法的 4 种分片机制

Table 2 Four sharding mechanisms based on hash algorithm

算法	特征	缺点
哈希取模分片算法	对节点的某个关键特征值进行 hash 运算后取模，根据取模结果将节点划分到对应分片	缺乏扩展性和自适应性
一致性哈希算法	先求出分片的哈希值，并将其配置到圆环上的第 0—232 号位置。采用同样的方法求出节点间的哈希值，并将其映射到相同的圆环上	分片状态信息的维护需要考虑一致性问题
跳跃一致性哈希算法	节点根据跳跃一致性 hash 算法被划分到不同的分片中	通常不具备很好的弹性，在节点的动态添加或移除时，可能需要重新分配数据或合约，这会导致不稳定性和复杂性增加
带虚拟节点的 hash 环	虚拟节点是在哈希环上与实际节点相关联的附加节点。虚拟节点的数量通常远远多于实际节点，以提高哈希环上的分辨率。目的是提升哈希环上的均匀分布，以确保数据和任务的分配更加均匀	对于无许可的区块链，因为节点没有固有的身份或外部 PKI 可以信任，所以必须提供一种有效的身份建立机制，以限制恶意节点创建的虚假身份的数量

可验证随机函数(Verifiable Random Function，VRF)是一种非对称加密算法中的哈希函数。所有节点使用私钥作为输入的一部分，运用零知识证明技术来生成随机数，并验证接受的随机性的正确性。如果输出结果的随机数小于预定义的阈值，节点可以被选为领导节点或委员会节点。利用 VRF 函数的可验证性可避免恶意节点伪造分片信息而企图进入到某分片，提高了网络分片的安全性。可验证随机函数 VRF 与一致性哈希算法相结合的节点随机分配方法[20]，在保证可验证随机性的同时利用一致性哈希算法的特点，节点的分配工作不依赖于某个委员会，且避免了分片结果在全网广播，保证了节点随机并且均匀地分配在各分片中。尽管节点无法预测自己会被分配到哪个分片，但是分片后每个分片内节点数量的减少可能导致一些潜在的安全风险。如恶意节点可能会更容易在较小的分片中集结起来(恶意节点占据了分片中超过 50%的算力，可以更轻松地对区块链进行攻击)，进而控制委员会，从而对分片内的交易进行攻击或者阻碍正常的交易确认过程。

OmniLedger[4]使用分布式 RandHound 随机数生成器生成的随机数作为节点分配的基础，而不是节点 ID。该函数的重要特征在于得到结果的计算过程无法并行计算，即无法加速，消耗的时间久，但得到结果后，验证该结果的计算量却又非常小。由 VRF 的领导者选举算法选举出 leader 节点，RandHound 随机数生成器提供了一种抗偏置的分布式随机生成协议，将所有节点随机分到某个分片中，以保证各分片的恶意节点比例均匀化。在随机数生成器协议中，进一步引入可验证随机函数，以其唯一性、抗碰撞性和随机性来产生领导者，并保证该领导者具有不可预测的鲁棒性。但是，攻击者可能试图偏向随机性，在诚实节点获得值之前，预测未来的随机数输出，或者欺骗第三方接受无效的随机数。上述这些方案既不能保证生成完全不可预测的随机值，也不能保证无论对抗行为如何都会生成值。

可验证延迟函数(Verifiable Delay Functions，VDF)的计算时间是固定的，并且无法通过任何手段加速或减慢计算过程，从而提供一个确定性的、无法被篡改的时间参考点，且计算结果是可验证的。具有固定的时间延迟的 VDF，使得攻击者无法在这个时间内确定随机数的输出。例如，在 PoW 共识算法中，矿工需要找到一个符合一定条件的随机数(也称为“nonce”)，以获得挖矿奖励。如果随机数太容易被预测或者被篡改，那么整个 PoW 算法就会失去可靠性和安全性。使用 VDF，可以将随机数的生成过程延迟一段时间(例如数小时)，使得攻击者无法在这段时间内确定随机数的输出。这样就可以有效地防止攻击者对随机数进行预测和攻击，从而提高整个系统的安全性和可靠性。但 VDF 的安全性依赖于对某些计算过程的时间延迟参数非常准确的估计，而在实际情况中很难获得参数的精度。

RapidChain 系统[5]中主要包含 3 个重要阶段，分别是引导启动阶段、共识阶段和重构阶段，如图 8 所示。

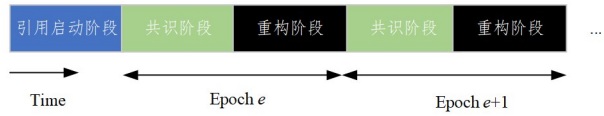

图 8 RapidChain 系统的 3 个重要阶段

Fig. 8 Three important phases of RapidChain system

其中，引导启动阶段是为了创建一个初始随机源，并随机选出一个特殊的委员会(称为参考委员会)，再由这个参考委员会的成员对节点进行随机分配，构成一个个分片委员会。在整个分片过程中只需要进行一次引导启动阶段。图 9 为 RapidChain 选举网络示意图。

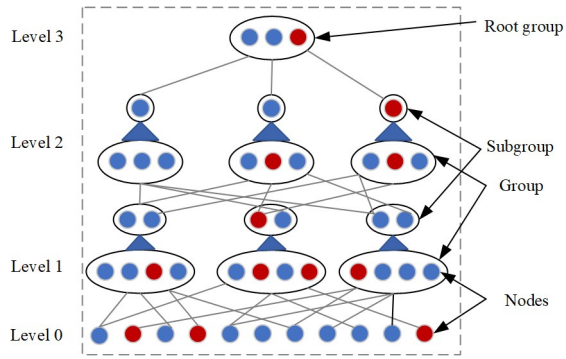

图 9 RapidChain 选举网络示意图

Fig. 9 Schematic diagram of RapidChain election network

具体步骤如下：假设分片配置环节初始节点集已经建立了身份，整个网络持续地从低一层的节点中构造一个随机二分图 $G(L,R)$，L 为节点(nodes)，R 为组(groups)。每个 group 内部运行一个分布式随机数生成算法(DRG)，生成一个无偏的随机值 s。然后每个节点把 s 和子集的 ID 进行一次哈希运算，哈希值落在某个区间内的节点广播宣称节点是被

子集选中的，小组内的其他节点都对这些(ID,s)进行签名，证明这些节点是被选中的节点。随后，这些选中的节点把自己的身份(包含刚才提到的证明)广播到整个网络中，选为 subgroup 成员，再由 subgroup 中的成员随机组合成更高一层的 group，被选中节点发送消息告知全部节点。重复上述过程，直到选出负责选择参考委员会成员的 root group，参考委员会完成所有节点的随机划分分片，构成一个个分片委员会。

上述委员会分片机制都需要设定其划分委员会的数量 k。若 k 设置过小，委员会数量较少，当整个网络节点数量激增时，每个委员会内的节点数量会过多，导致每个委员会的交易处理效率较低；反之，若 k 设置过大，委员会数量较多，节点数量不变的情况下，片内节点数量较少，诚实节点的数量被分散，安全性较差。基于随机函数的委员会随机分片机制依赖于领导节点。分布式环境下领导节点的选举会产生计算和通信时延，特别是在节点数量较多的情况下，会影响委员会机制的效率。

3)基于地理位置的分片机制。Sharper[21] 考虑到人类活动的地域限制，日常生活中的大多数交易都是在同一国家/地区进行的，且地理位置较近的节点之间的通信延迟较低，便于交易和区块的传播，因此将各个节点的地理位置纳入区块链分片策略也是解决分片区块链可扩展性问题的一种方法。文献[22]将每个分片建立在一个区域代码上，每个节点仅由特定分片根据区域代码处理。同一区域内的网络延迟相对较小，因此可以更快地处理交易。Chai[23] 将各个医院看成一个个区块链上的节点，医院产生的数据通过区块链进行存储，并且通过各个省市的地理位置进行分片，这样在保证了安全存储数据的同时，可以解决信息孤岛问题。尽管基于地理位置的分片方法有一些优势，但这样的节点分配方法不能平衡每个分片中的节点数量，容易受到对手的攻击。

表 3 对基于节点分片配置的 3 种静态优化方法进行了比较。采用单纯的静态优化方法分配节点，仅仅使分片节点数量在某种程度上保证了均衡，只能为分片提供概率安全性，忽略了节点之间存在的性能差异与协同事务，虽然提高了区块链网络性能，但会出现单点过热的问题，导致单个分片阻塞并降低整个系统的吞吐量，更不适用于动态变化的复杂环境。综合考虑区块链系统的节点负载、节点信用、网络质量、交易速率等多种因素的动态优化分片配置方法可以保持所有分片总体的均衡性，避免聚合情况的发生。

表 3　3 种静态优化方法的比较

Table 3　Comparison of three static optimisation methods

静态优化方法	实现方法	优点	缺点
hash 算法	hash 映射	简单易操作，延迟较低	限制了分片数量的动态性，故障概率高
随机分片机制	可验证随机函数(VRF) RandHound 随机数生成器 可验证延迟函数(VDF) 分布式随机数生成算法(DRG)	简单易操作，延迟较低	领导节点的选举会产生计算和通信时延，特别是在节点数量较多的情况下，会影响委员会机制的效率
地理位置分片	将地理上距离比较相近的节点分在一个分片	通信延迟较低	节点数量失衡，容易受到对手的攻击

4.1.2　节点分片的动态优化方法

动态优化方法，即在进行区块链分片时，根据不同的情况选择不同的分片策略。动态优化方法更适合变化的区块链环境。

1)信誉积分分级分片策略。大多数当前的分片方案假设所有节点都是同构的，但是每个节点在硬件和网络方面是不同的。可能只有部分节点会积极参与共识，而其他节点则不活跃。具有更多非活跃节点的分片可能更容易受到接管攻击者的攻击。考虑筛选出信誉值高的节点参与共识，在分片共识开始之前，根据节点所处信誉等级进行信誉分片，决定节点在哪个分片有投票权，从而保证了各分片内共识节点的数量平衡以及节点分片的不可预测性和安全性。每个节点的声誉会根据其在本轮中的行为进行更新。因此，节点表现出的算力越高，则其声誉的提升就越多；表现出的算力越低，其声誉的提升就越少，甚至可能降低。同时，被成功检举的邪恶节点会在这一阶段得到惩罚。信誉分片示意图 10 所示。

Repchain[5] 提出了一种信誉值方案，以鼓励诚实、有能力的节点做出更多贡献。其信誉值是基于节点对共识的贡献程度来计算的。在每个时期的开始，节点按信誉值排序，然后将节点依照该排序依次分配给含有节点数量最小的分片。每个分片中信誉度最高的节点被选为领导者，负责分片内共识和处理跨分片交易。领导者会比其他节点更快地积累信誉分数，这给予了它们正激励。该方法可以保证分片中节点的数量和质量相对均匀。但是，对手可以通过控制固定数量的节点，假装是正常节点，直到其中一个被选为领导者，然后发动攻击。因此，该系统很难抵御缓慢适应的对手。文献[24]提出了一种基于信誉驱动的动态节点安全分片共识模型，该模型通过不同的节点配置，一方面降低了异常节点成为主节点的概率，另一方面保证了分片的可靠性，提高了区块链的吞吐量。

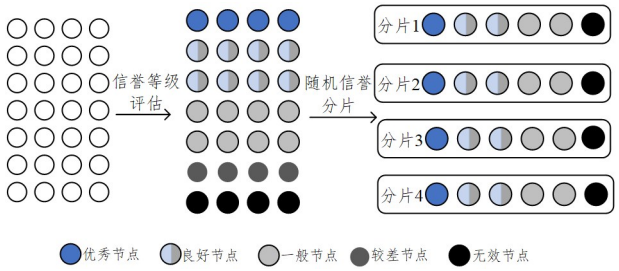

图 10　信誉分片策略

Fig. 10　Credit sharding strategy

Cycledger[25] 在基于信誉分片策略的基础上，提出了一种基于信誉与可验证随机函数(VRF)相结合的节点分配方案，用来评价网络中每个节点的算力大小以及诚实程度。CycLedger 中有 4 种类型的节点：中心裁判委员会节点、组长节点、监察员节点和剩余的非关键节点。整个网络的结构如图 11 所示。

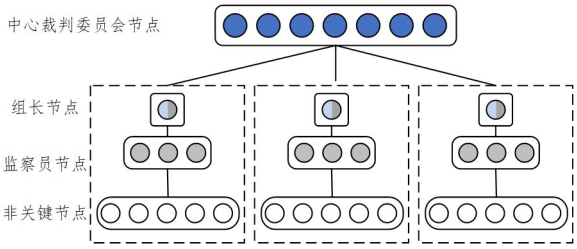

图 11 Cycledger 网络结构图

Fig. 11 Diagram of Cycledger network structure

在每一 epoch 中，会产生一个中心裁判委员会负责管理其他所有小组并产生最后的区块。其余所有节点被均匀分成若干个小组，每一个小组由一个组长、若干个监察员和其余群众构成。每个小组中信誉最高的节点被选为组长，组长负责收集与相应分片用户相关的交易并统筹组员的意见，而后将最终决定提交中心裁判委员会进行审核。每组的监察员负责监督本组组长的行为，一旦组长做出违反协议规定的行为，诚实的监察员会向中心裁判委员会进行检举，若检举通过，则将原有组长换下，更替新的组长（诚实的监察员之中的一个）。因此，监察员也被称为候选组长。一组中的其余节点则只需要存储相关交易，负责进行群体决策。一个节点算力越高，其声誉越高，获得的奖励也就越多。而一个被确定作恶的节点（被成功检举的组长）的声誉会大幅下降，进而导致其收益降低。但中心裁判委员会中的节点需要存储所有其他委员会交易集，以进行验证和转发。

Free2Shard[26]是一种用于同步网络的基于声誉的动态分配策略，采用动态自分配（DSA）算法，节点随机分配，却忽略了隐私保护。文献[27]提出一种基于信任的分片分布（TBSD）方案，将网络中潜在的恶意节点分配给不同的分片，防止恶意节点对单个分片的共识产生主导性影响。SL-Chain[28]依靠声誉建立了确认委员会，该委员会允许快速确认区块，而无需分叉，通过在分片之间协同工作进行区块验证，以避免因单个分片被对手控制而出现的数据不一致。

信誉分片能够保证各分片内节点的等级分布近似相同，如果单分片内出现恶意节点可以联合作恶成功的情况，则说明参与共识的大多数节点都是恶意节点，系统已经崩溃。

2）遗传算法分片策略。使用遗传算法可以最小化恶意节点分配在同一个分片中的概率。考虑分片区块链系统中节点的计算能力、恶意节点的概率以及节点之间的传输速率等不同的情况，找到响应网络状态的最佳分片区块链系统参数。为了避免随机分片导致的单分片恶意节点集结，基于遗传算法（Genetic Algorithm，GA），根据节点的信誉值进行分区，使得每个分区的信誉值差异最小化，实现了一个比较完善的信誉平衡。但是，该策略在分片过程中可能会耗费很长的适应和计算时间，造成区块链系统分片过程效率低下。

3）深度强化学习分片策略（Deep Reinforcement Learning，DRL）。深度强化学习[29]是把深度学习与强化学习相结合的一种人工智能方法。深度强化学习可以从以往的经验中学习区块链分片系统的特点，并根据当前的网络状态采取合适的分片策略，以获得长期的回报。Skychain[30]利用深度强化学习（DRL）对区块链系统进行动态分片的方案中，智能体与区块链系统产生的数据会存储到经验回放池，通过不断地训练寻找最优的分片方案。通过采用延迟的分析方程和深度强化学习，能有效保证在动态环境下的系统性能和安全性的均衡。文献[31]提出了一种利用深度强化学习的自适应分片机制来自动选择车辆分片的参数，降低了智能汽车在主链和子链之间的交互产生的高通信成本，用于智能车辆之间的数据交互，解决了基于区块链的单一车辆网络吞吐量有限的问题。

Lin 等[31]使用系统分片产生的历史数据得到最优的分片策略，使用深度强化学习，而不需要建立系统去分析模型，提高了区块链的性能。

基于深度 Q 网络算法（Deep Q Network，DQN）算法，文献[32]提出了一种基于深度 Q 网络分片的区块链（Deep Q Network Shard-based Blockchain，DQNSB）方案来获取动态环境中的最佳配置方案。为了保证分片方案的稳定性，估计当前恶意节点的占比情况，根据网络状态自适应调整区块链参数，DQNSB 动态地找到了大规模区块链的最佳吞吐量配置。该方案具有更高的吞吐量，且保持了较高的安全级别。但是，在区块链分片中使用的深度强化学习算法中，行为空间随着行为维数的增加而增加，导致深度强化学习算法效率降低，神经网络难以顺利训练。竞争 Q 网络算法（Dueling Deep Q Network，Dueling DQN）[33]是经典的深度 Q 网络算法的改良算法，进行系统的最终分片方案决策。由于设置的状态变化依赖状态转移矩阵，不依赖智能体的动作，因此计算动作的状态函数比计算动作的价值函数意义大，即采用 Dueling DQN 比 DQN 好。

4）机器学习动态优化方案。根据区块链网络中的交易历史记录对账户进行分片，确保片内交易占据一定比例、跨片交易所占比例降低的分片策略，依然保证各分片交易划分相对均匀。

Wang 等[34]使用 K-medoids 聚类算法将所有节点划分为多个节点簇，每个节点簇构成一个分片，但其计算复杂度高，且只用于数值型数据。Bai 等[35]基于复杂网络社区划分算法[36]改进区块链网络分片算法，以提高区块链网络的吞吐量，缩短分片时间，减少分片时间和各分片内区块的广播时间。但是，社区划分算法不限制社区的大小，因此可能会产生非常大的社区，导致分片工作的负载不平衡指数较高。

5）基于权重矩阵动态优化方案。文献[37]提出一种基于账户加权图的交易分片算法。首先，从数据分片的角度建立基于账户的交易分片模型。其次，基于该模型，构建以账户为节点，以账户间交易频率为权重的账户加权图，以获取区块链长期累积的交易数据。采用社区发现算法，根据账户之间的关联关系，选择模块化增益最大的账户进行合并，从而初步形成多分片区块链。最后，通过拆分和合并对多分片区块链进行调整和重建。有效降低了跨分片交易占比，并最大限度地减少了跨分片交易延迟。

文献[38]基于动态奖惩机制（MaOEA-DRP）的多目标优化算法，优化分片验证效度模型，使恶意节点均匀分布。但该方案只考虑各分片的权重在目标函数中均衡分配，而不是分片之间的工作负载平衡。分片之间的工作负载平衡对于分片至关重要，是提高吞吐量、降低确认延迟和

保证交易顺序公平性的关键。

4.1.3 节点配置到多分片方案研究

传统的分片机制中，一个节点只能在一个分片中。而一些分片机制中，节点可以选择参与多个分片的处理并维护它们的分类账。如图 12 所示，多色圆圈表示该物理节点虚拟化后同时在多个分片内参与共识，而单色圆圈表示仅参与单个分片的共识过程。本小节主要介绍当前单节点维护多分片的方法研究。这类研究一般是将每个物理节点映射为多个虚拟节点，结合分布式随机协议与可验证随机函数，使单个节点可以维护多个分片，同时参与相应分片的共识。

另一种方法是按照数据区间范围进行分片。物理节点在 hash 环上的位置是动态变化的，这与一致性哈希非常类似。如果一个节点负责一个区间，区间范围与一致性 hash 类似；如果一个节点负责多个区间，区间范围与带虚拟节点的 hash 环类似。Ostraka[13]是一种非民主环境中的扩展节点架构，其中节点可以同时加入不同的分片。它的延迟和吞吐量分别随分片数量线性增加而增加。Pyramid[39]是第一个具有分层分片共识的区块链系统。通过将节点配置到多个分片中，允许各个分片彼此重叠，使得某些分片（称为桥接分片）存储多个其他分片的区块，充当分片间桥梁的作用。桥接分片可以直接验证跨片交易，增强了跨分片交易的处理能力，提升区块链系统的事务吞吐量，降低事务确认延迟。

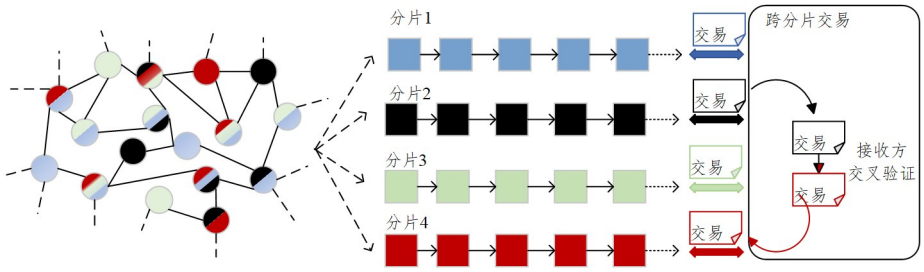

图 12 分片系统示意图

Fig. 12 Schematic diagram of slicing system

BrokerChain[40]基于动态状态划分策略提出一种新的跨分片协议，以提高跨分片交易处理的效率。在进行状态划分的过程中，系统允许一部分普通用户通过自愿抵押一定资产来充当“中间人账户”。“中间人账户”的状态会被系统分割成 2 个或多个部分，分别存储在 2 个或多个分片中，从而参与到若干个跨分片交易的协调中。该文提出的跨分片协议可以减少跨片交易延迟，提高跨片交易执行效率。

为了保护系统免受接管攻击，Monoxide 引入了连弩挖矿（Chu-ko-nu Mining）算法。该算法允许节点同时在多个分片中挖掘新块，从而在经济激励方面分散恶意节点的计算能力。把所有节点的物理算力都放大 n 倍得到有效算力。诚实节点一般都会分散自己的算力到各个分片中以获得好的收益，因此可以同时在多个分片内出多个块，而攻击者一般是只攻击一个分片。这样，便放大了诚实节点的算力，使其与攻击者的算力相等。

4.2 基于交易的分片策略

分布式账本有基于交易和基于账户的两种交易模型。基于交易的方式是将所有交易按照其类型或者其他属性（例如交易的输入地址）映射到各个分片，每个分片只需处理某些特定类型或属性的交易；基于账户的方式是将所有交易按照其涉及的账户进行分类，每个分片只需处理某些特定账户的交易。在分片系统的交易分发过程中，不同的交易模型会采用不同的映射机制来将交易映射至分片。映射机制会影响分片处理的性能，使得系统中存在片内和跨片两类交易。需要处理过量交易的分片被称为热分片（Hot Shard），只需处理少量交易的分片被称为冷分片（Cold Shard）。对于热分片，由于存储在分片中的账户发起大量交易时，分片的工作负载将超过其最大处理能力，片内交易的确认延迟较大，导致分片内和跨分片的交易暂时阻塞，可能成为整笔跨片交易处理过程中的性能瓶颈；冷分片由于接收的交易数目少，区块内的交易填充率低，导致分片内节点计算和网络等资源的浪费。

交易分片是将区块链中的主要工作负载划分到不同的分片进行并行处理。跨分片交易的开销最终可能抵消分区的益处。交易分片要求最大限度地减少跨分片交易的生成，并且使得每个分片的交易负载尽可能均衡。

4.2.1 交易分片的静态优化方法

monoxide 根据发送方所在的分片决定交易的分片，就能简单验证发送方是否有足够的资金，但可能会导致所有区块链分片之间的交易分配不平衡；并且其只能实现一个地址给多个地址转账，不能实现两个地址给其他地址转账以及多个地址给多个地址转账的情况。

SSChain[17]将原始比特币与分片 id 连接起来，形成一个复合地址，其中最后 2 个字节指定目标分片 id，便于交易路由。由于每个地址都包含目标分片 id，因此很容易找到交易的源分片和目标分片。地址结构如式(2)所示：

$$Address = Bitocin\ Address : Shard\ ID(2\ bytes) \tag{2}$$

大多数早期的研究将产生的交易随机地分配给分片中节点，采用了根据交易散列或参与者地址随机分配的原则，这导致大多数交易都变成了跨分片交易，通过交易分片的动态优化方法可减少跨片交易。

4.2.2 交易分片的动态优化方法

基于交易分片的动态优化方法，最近的研究集中在上下文感知方法上，即在事务被划分之前知道分片的当前状态，从而在源头上减少跨分片事务。Brockerchain[40]提出了一种事务分区代理分片系统，实时分析其中所有客户端交易事务的相关性，将关联度高的事务分配到同一分片，以减少跨分片事务的发生。然而，这种集中式体系结构会使代理分片成为整个系统的可伸缩性瓶颈。文献[41]提出的方法是将通过

跨分片交易访问的高度相关的数据动态地重新定位到同一个分片中。此外，将两个或多个高度相关的分片自适应地合并为单个分片，或者将单个分片拆分为更小的不相交分片，通过智能合约实现对动态分片组织中数据历史记录的跟踪，以充分利用并行分片，在动态状态变化时保持账本的一致性。EfShard[42]基于贪心分配算法来决定状态的迁移，将高度关联的状态数据分组到同一个分片中，以减少跨分片事务的比例，并将状态数据分发到负载相对较低的分片上，以均衡工作负载，从而提高性能。TxAllo[43]将交易分配问题表述为图上的社区检测问题，即无向和加权交易图上的图分区问题。该图可以捕获区块链地址之间的交易频率，用于动态推断账户及其关联交易的分配情况。

4.3 重分片策略

分片技术减少了区块链内参与共识的节点数量，但降低了单一分片的安全性。区块链系统中即使有节点身份验证机制，也仍然避免不了恶意节点的存在；而诚实节点长期处于某一分片可能会遭到恶意节点的腐败，进而转变为恶意节点，或者恶意节点可以通过不断涌入单一分片，使得恶意节点的比例超过该分片的安全阈值（如 PBFT 中的 1/3）并控制该分片，这将破坏整个系统的有效性和安全性。因此，分片区块链系统需要定期更新分片内成员，通过引入重分片机制，系统会周期性地对系统内的节点进行分片重构，以确保对手控制的节点数量始终低于安全阈值。

分片重构需要考虑 3 个关键问题。首先，必须确保重新配置后的每个分片中的诚实节点的数量超过安全阈值；其次，系统应该能够在重新配置期间正常处理事务；最后，在重新配置完成之前，破坏攻击的行为不会成功。

分片重配置的方式分为全重分片配置和部分重分片配置两种。全重分片配置指对所有节点重新进行委员会划分，对系统所有节点进行重新分片，这要求系统中所有节点都重新启动进行存储迁移等操作，造成大量的性能损耗；部分重分片配置是从原有分片中取出一部分节点并与其他分片中的节点进行交换，当有新节点想要加入时，验证并接收新加入的节点后通过一定的重构规则将新节点进行分配。

4.3.1 全重分片策略

对所有节点进行重新分配，既能彻底防止节点之间进行作恶，也能将新节点加入分片中。分片重配置策略和节点分配策略通常使用相同的方法。下面将介绍几种全重分片配置方法。

Elastico[3]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，由最终委员会计算出 Randomness 函数结果，以供下一轮的重新配置阶段使用。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。

Etherscan[15]每隔一个周期（一个周期是产生 32 个区块的时间）通过信标链将网络中的节点重新分配到不同的分片，以提高安全性和避免任何单一分片的集中化。信标链是 Etherscan 的核心组成部分，其主要作用是实现和管理 Etherscan 网络中的权益证明（Proof of Stake，PoS）机制。信标链通过 RANDAO 和可验证延迟函数 VDF 计算出的随机数将所有节点重新分配到不同分片。RANDAO 是一种生成随机数的方式，其有效运行需要引入防作弊机制。VDF 函数保证所有人同时给出答案，信标链负责连接主链以及管理各个分片，通过随机性选择分配节点可以避免节点的聚集。

上述分片区块链系统均采用静态优化策略。下面介绍几种动态优化策略。

Mizrahi[44]提出在每个纪元结束时动态调整事务划分规则，在下一个纪元将密切相关的地址映射到相同的分片，并在所有节点之间达成共识。虽然它保持了去中心化，但这种方法的效率明显低于实时分区。上述方法既不能实现去中心化，又不能做到有效性的交易划分。解决该困境的方法是引入深度学习，探索更多与交易相关性相关的特征，从而提高单一调整的有效性。BrokerChain[40]使用了一种新的动态规划（Dynamic Programming，DP）调整分片状态的新架构。与强化学习类似，其根据历史信息构建账户状态图，并根据图对分片的状态进行动态调整与重配置。

文献[45]通过引入动态区块链分片机制，以实现按需创建分片或关闭分片。少数用户通过主链上的专用智能合约调用来重新配置分片的数量和每个分片大小，在运行时更改分片的数量，这不仅增强了分片重新配置的安全性，还使其与任何其他区块链数据一样具有内在的透明性。因为不需要完全同步通信，所以该协议非常适合开放的网络，且性能随着分片数量的增加而线性增加。

虽然全重随机分片配置能够最大程度地保证分片后区块链网络的安全性，但是在重配置的过程中，整个网络对于交易的验证停滞，全网都要在重配置前后进行新旧账本的交接，并为分片重新进行计算和广播，都大幅降低了整个区块链的性能。

4.3.2 部分重分片策略

考虑到全重分片配置所带来的停机时间和通信开销，一些区块链分片系统在分片重配置阶段通常只更换部分节点。

OmniLedger[4]实现了一个随机替换方案来对节点进行重分片配置，通过设计了一种灰度化处理方法，建立一个专门用于管理身份的区块链，在分片中通过随机方式选出部分节点用于下一个 epoch，进行重组优化，剩余节点会继续进行交易处理，这使得将当前 epoch 的交易处理和下一个 epoch 的分片重组并行，节省了 epoch 切换的时间开销，提升了系统性能。在 OmniLedger 中，需要限制移出节点的个数少于片内节点数量的 1/3，从而使得移除节点后的片内剩余节点可以保证 BFT 共识的安全性。该方案中，重分片配置的节点以及新加入分片的节点会造成数据迁移，产生很大的延迟，而且扩展性是原来一半，并不适合高度自适应的对手。

RapidChain[5]提出了一种基于布谷鸟规则（Cuckoo Hashing）的轻量级重新配置协议，其中每个时期只允许恒定数量的验证者在委员会之间重分配。布谷鸟规则是只对部分节点采用 hash 函数，将其映射到[0，1）区间的随机数，再将[0，1）区间划分为 k 个子域，对应于 k 个委员会。当有新节点加入某一子域时，为保证子域之间节点数量的平衡，新节点位置周围的临近节点会被移除到其他子域。这种机制有效限制了受影响的节点数量，仅需要部分节点重新启动并进行存储

迁移，节省了系统重组带来的性能开销。与 OmniLedger[4] 相比，这种设计产生的开销更少，并且允许更频繁的历元重新配置，以抵抗更高适应性的对手，但它们也缺乏严格的安全证明。

由于每个节点只保留当前分片的账本，因此重分片配置涉及的节点需要下载它们被重新分配到的新分片的账本，此过程被称为数据迁移。在进行部分重分片配置的过程中，除了需要进行迁移的节点外，分片内的其他节点仍然正常进行交易验证，从而大幅降低了重配置过程对区块链性能的影响。新节点加入分片时，必须确保节点有足够的时间与分片的状态同步，否则，新加入的节点将拒绝处理交易。

4.3.3 无需重分片策略

在许可链中，通常是一个已知的、受信任的参与者集合，而不是像非许可区块链那样的匿名节点。这意味着许可链中的网络结构和网络容量可以事先规划实现可扩展性，而不需要频繁地重新分片。但不需要重新分片配置并不意味着不需要关注数据管理和性能问题，而是强调了对可控制环境中的合适策略和技术的重要性。

SSchain[17] 涉及两层结构而不需要周期性重新配置分片，其中节点可以基于共识机制加入一个或多个分片。

当有新节点加入时，新节点可以根据式 $GPH(BR=BlockReword, HP=HashPower, BI=BlockInterval)$ 的增益函数选择目前收益最高的分片加入，而在当前分片的收益较低时可以退出并加入到收益高的其他分片。GPH 函数综合考虑分片出块收益、出块间隔以及当前哈希算力，而哈希算力的分配又综合了对主链算力和分片算力的分配，既体现了对链安全性的考虑（即对算力的宏观分配），又充分考虑到了用户的个人意愿。GPH 函数如式(3)所示：

$$\frac{BR(root)}{BR(shard)}=\frac{HP(root)*BI(root)}{HP(shard)*BI(shard)}$$
$$GPH=\frac{BR}{BI}PresentHP \tag{3}$$

Monoxide 根据节点地址，采用固定的分片配置，不需要定期重新配置分片，同样允许节点自由选择分片，并通过激励机制保护系统的安全性。然而，激励机制的安全性是建立在经济行为人理性假设的基础上的，需要更系统的安全性证明。否则，由用户决定自己映射到哪个分片中，攻击者可以通过故意创建很多的地址生成特定的分片映射的地址，让这些地址都在某个分片内执行，造成某个分片负荷非常大。

表 4 对本节所描述的重分片策略进行了对比分析。相较于全重分片配置和部分重分片配置方式，自由选择重配置方案能够通过人为操作使得整个区块链网络达到收益最大化的动态平衡，但是其对恶意行为的抵御能力不如区块链系统调控下的重配置方案。

表 4 重分片策略的对比分析

Table 4 Comparative analysis of resharding strategies

配置方案	特征	常用策略	缺点
全重分片配置	对所有节点进行重新分配，既能彻底防止节点之间进行作恶，也能将新节点加入分片中	一致性哈希算法、随机重构策略、深度强化学习、动态规划等	通常需要系统的停机或维护时间，以便执行必要的更改，这可能导致分片系统不可用，对业务造成影响
部分重分片配置	将部分分片节点随机进行重分配，降低开销，减少重配置过程的等待时间	滑动时间窗规则、灰度化处理、布谷鸟规则等	当节点数量增加时，广播和收集签名将花费巨大的通信带宽和时间，从而影响整个区块链分片的效率
无需重分片配置	许可链内无匿名节点，不需要重新分片配置，只需考虑新节点的加入	星型架构、增益函数、激励机制、节点自由选择分片法等	通常需要更多的计算和存储资源来动态适应负载的增加，可能导致性能下降

5 现有分片技术方案分析

本文从区块链系统的分片策略、是否需要重分片、架构类型、分片数量、分片大小与吞吐量 6 个方面对主流的分片区块链系统进行分析，对比结果如表 5 所列。分片区块链系统通过改善不同的分片流程部分，不断进行优化。通过静态优化和动态优化方法进行不同的分片策略，不同的分片策略适用于不同的应用场景和网络需求。分片区块链系统是否需要重分片步骤，可能涉及增加或减少分片的数量，改变分片之间的节点或交易分配，甚至重新设计整个分片结构。

表 5 分片区块链系统的比较

Table 5 Comparison of sharding blockchain systems

区块链分片系统	分片策略	是否需要重分片	架构类型	分片数量	分片大小	吞吐量
Monoxide	节点地址 hash	×	平行	$2^{10}\sim2^{18}$	$10^2\sim10^4$	1.23～2.56 Mtps
Elastico[3]	参考委员会	√	星型	小于 10^2	小于 10^2	45 ktps
OmniLedger[4]	RandHound＋VRF	√	星型	小于 2^6	$2^2\sim2^{10}$	28.8 ktps
Rapidchain[5]	VSS＋拉格朗日插值	√	平行	小于 2^8	$(2^2-1)\sim2^8$	128 ktps
Ethereum 2.0[15]	RANDAO＋VDF	√	星型	小于 2^9	小于 10^2	134 ktps
Chainspace[12]	—	×	平行	小于 10^2	小于 10^2	小于 400 tps
Repchain[5]	Randhound＋VRF	×	星型	小于 2^{11}	小于 10^2	5682 tps
SSchain[17]	分片 id＋GPH	×	星型	小于 10^2	小于 10^2	6500 tps
Sharper[21]	地理位置	×	平行	小于 10^2	小于 10^2	27000 tps
BrokerChain[40]	节点地址	√	星型	小于 10^2	小于 10^2	352 tps

其中，√表示满足特征；×表示不满足特征；—表示未定义。

平行架构提供了更高的并行性和吞吐量，适用于大规模交易处理的场景，例如金融交易、供应链管理等，但可能需要更复杂的网络管理和通信协议。星型架构提供了更好的一致性和集中管理，适用于对一致性要求高、网络结构相对简单的

场景，例如政府或企业内部的应用，或者对网络拓扑结构有严格要求的场景。在实际应用中，可能也会出现混合使用这两种架构的情况，以满足不同场景的需求。分片数量和分片大小应该合理设计，提高分片区块链网络的整体性能。更多的分片可以并行处理更多的交易，但也可能增加网络通信和同步的复杂性。分片应足够小，以确保分片内的交易和智能合约能够快速处理；同时分片数量不宜过多，以避免过多的管理和通信开销。

5.1 性能评价分析

分布式账本性能评估是一个系统的重要评价指标，本节从扩展性和可靠性两个方面（具体为吞吐量、时延、通信开销、节点均衡性、随机性、安全性和是否可以跨片智能合约等方面）定性、定量分析现有的区块链分片系统。图 13 给出了性能评估的分类结果，表 6 对现有几种主流区块链分片系统性能评估进行了分析。

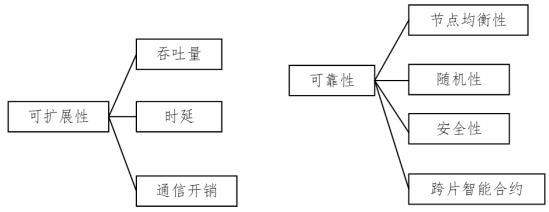

图 13 区块链分片技术性能评估指标

Fig. 13 Performance evaluation metrics of blockchain sharding technology

表 6 分片区块链系统性能评估总结

Table 6 Summary of sharding blockchain system performance evaluation

出版年份	系统名称	类型	可扩展性			可靠性分析			
			吞吐量	时延	通信开销	节点均衡性	随机性	安全性	跨片智能合约
2016	Elastico[3]	交易	$O(n/\log n)$	$O(1)$	$O(m^2)$	√	√	×	×
2017	Zilliqa	DApps	$O(n)$	—	$O(m^2)$	√	×	×	√
2017	Chainspace[12]	DApps	$O(n/m)$	$O(1)$	$O(m^2)$	√	×	√	√
2018	OmniLedger[4]	交易	$O(n)$	$O(N)$	—	√	√	×	×
2018	RapidChain[5]	交易	$O(n)$	$O(1)$	$O(m^2)$	√	√	×	×
2018	Ethereum 2.0[15]	DApps	—	—	$O(m^2)$	√	√	×	×
2019	SSchain[17]	交易	$O(n)$	$O(N)$	$O(m^2)$	√	√	×	×
2019	Monoxide	交易	$O(n)$	$O(\log n)$	$O(m)$	√	×	×	×
2020	polkadot[16]	DApps	—	—	—	√	—	—	—
2021	Sharper[21]	交易	$O(N)$	$O(N)$	$O(m^2)$	×	√	—	×
2021	Meepo[46]	交易	$O(n)$	$O(n)$	—	√	×	×	√
2021	Fleetchain[47]	交易	—		$O(m^2)$	√	×	×	×
2022	pyramind	—	$O(N)$	$O(N)$	$O(m^2)$	√	√	×	√
2022	brokerchain[40]	交易	$O(N)$	—	$O(n^2)$	√	×	×	√
2022	Free2Shard[26]	交易	$O(N)$	$O(1)$	$O(\log N)$	√	√	×	×
2023	Light-PerlChain[48]	交易	$O(n^2)$	—	$O(3n+n\log N)$	—	√	√	×
2023	GradingShard[49]	交易	$O(n/m)$	—	$O(n)$	√	×	√	×
2023	LB-Chain[50]	交易	—	$O(1)$	—	√	√	√	×
2024	X-Shard[51]	交易	$O(N)$	$O(n)$	$O(n)$	×	×	√	×
2024	Estuary[52]	交易	$O(n)$	$O(N)$	—	√	×	×	×

其中，√ 表示满足特征；× 表示不满足特征；— 表示未定义；N 表示参与节点的总数；m 表示分片的数量；n 表示分片内节点得数量。

吞吐量：吞吐量的 O() 表示描述系统或算法在单位时间内能够处理的操作或事务数量的增长趋势。吞吐量是区块链网络每秒可处理交易的数量，其可作为衡量整个区块链网络性能的指标。

时延：时延的 O() 表示描述系统或网络中所需处理的操作或事务的平均时间的增长趋势，主要体现在共识阶段，确认交易已被包括在区块链中的时间内。时延模型是在区块链网络所使用的共识协议的基础上建立的，可用于评估和比较不同系统的性能和处理能力。

通信开销：通信复杂度 O() 是一种用于描述算法通信操作数量增长趋势的方法，可以评估和比较不同算法的通信开销。

节点均衡性：将节点均衡分布情况作为指标，分析分片数量和节点数量对节点均衡分布情况的影响。

随机性：随机性在确保恶意节点在不同分片中的公平分布方面起着至关重要的作用，可以降低攻击者获得单个分片控制权的概率。

安全性：分片方案应该应用有效的方法来防止恶意节点跨分片勾结以损害用户数据和身份的隐私。是否能减轻集中式攻击带来的威胁是衡量一个分片区块链系统安全性的重要方式。通过采用超几何分布对分片区块链系统的安全性进行分析，得到分片系统被恶意节点破坏的可能性。

跨片智能合约：区块链分片系统需要实现跨片智能合约，因为这有助于提高分片系统的功能和灵活性，解锁更多的应用场景，并提升区块链的整体性能。

5.2 分片技术的挑战与未来展望

综上所述，分片是解决区块链可扩展性问题最有前途的技术之一。与成熟但缺乏可扩展性的现有区块链解决方案相比，分片技术仍处于起步阶段。虽然分片在理论上有可能实现接近线性的可扩展性改进，但现有的区块链分片方法没有考虑分片之间的分片信任差异、通信时延差异和节点数差异，这往往会增加区块链故障的风险。未来的研究可基于机器学习或深度学习的节点划分策略，将不同信任级别的节点划分到合适的分片上，使不同分片具有几乎相同的信任度，从而提高分片的可靠性。

在分片设置阶段，节点选择、节点分配、事务划分和分片重新配置都依赖于随机数。现有的一些方案不能保证随机数生成的无偏性和有效性，有的方案依赖可信初始化进行引导，这在实践中很难实现。因此，随机数生成方法仍需进一步

研究，未来可使用可验证延迟函数等密码学原理和算法来生成随机数，从而提高随机数生成的安全性和效率，并且抵御各种攻击，如对随机数的预测攻击和推导攻击等。

如何缩短分片重配置带来的延迟仍然是难题，未来可以利用可信执行硬件减少节点选择时间来降低获得节点身份的时间成本。

智能合约对于区块链在金融以外的领域广泛应用至关重要，目前大多数关于非许可链分片区块链的研究都是基于UTXO模型，但该模型不支持智能合约。即使是基于账户的分片许可区块链中支持智能合约的研究[53]，也没有显示出资产转移之外的其他应用场景。这与提出的分片技术的最初目的相去甚远，分片技术的最初目的是提高区块链的可扩展性，以使其有更广泛的应用。因此，研究支持NFT和合约调用等复杂应用的分片区块链是未来的重要方向之一。

结束语 本文从分片结构、分片机制、重分片策略等几个方面，对区块链分片相关研究工作进行了较为系统的综述，分析了各种方法的优点与不足，总结了区块链优化技术的方法，分析了存在的问题，最后思考了区块链分片技术未来的发展方向。

参 考 文 献

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

[2] HAN R, YU J, LIN H, et al. On the Security and Performance of Blockchain Sharding[J]. Cryptology ePrint Archive, 2021, 2021: 1-15.

[3] LUU L, NARAYANAN V, ZHENG C, et al. A Secure Sharding Protocol For Open Blockchains[C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 17-30.

[4] 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 (SP). 2018: 583-598.

[5] 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, NY, USA: Association for Computing Machinery, 2018: 931-948.

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

[7] LI Y, WANG J, ZHANG H. A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces[J]. Journal of Network and Computer Applications, 2023, 217(8): 1.1-1.19.

[8] HASHIM F, SHUAIB K, ZAKI N. Sharding for Scalable Blockchain Networks[J]. SN Computer Science, 2022, 4(1): 2.

[9] XU Y, SHAO J, 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): 34: 1-34: 27.

[10] CHEN R, WANG L, PENG C, et al. An Effective Sharding Consensus Algorithm for Blockchain Systems[J]. Electronics, 2022, 11(16): 2597.

[11] WANG K Y, JIANG X, JIA L P, et. al. Throughput Model of Starlike Sharding Structure for Blockchains and Its Applications [J]. Journal of Software, 2023, 34(9): 4294-4309.

[12] AL-BASSAM M, SONNINO A, BANO S, et al. Chainspace: A Sharded Smart Contracts Platform[J]. arXiv: 1708.03778, 2017.

[13] MANUSKIN A, MIRKIN M, EYAL I. Ostraka: Secure Blockchain Scaling by Node Sharding[C]// 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE. 2020: 397-406.

[14] CAI Z, LIANG J, CHEN W, et al. Benzene: Scaling Blockchain With Cooperation-Based Sharding[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 34(2): 639-654.

[15] BEZ M, FORNARI G, VARDANEGA T. The scalability challenge of ethereum: An initial quantitative analysis[C]// 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE). 2019: 167-176.

[16] BURDGES J, CEVALLOS A, CZABAN P, et al. Overview of Polkadot and its Design Considerations[J]. arXiv: 2005.13456, 2020.

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

[18] XIAO F, LAI T, GUAN Y, et al. Application of Blockchain Sharding Technology in Chinese Medicine Traceability System [J]. Computers, Materials & Continua, 2023, 76(1): 35-48.

[19] SUN E Y, LIANG J M, LIU J B. Blockchain Sharding Optimization Scheme Based on Virtualization[C]// Intelligent Information Processing Industrialisation Branch, China High-Tech Industrialisation Research Association. 2022.

[20] WANG J, WANG S, ZHANG Q, et al. A two-layer consortium blockchain with transaction privacy protection based on sharding technology[J]. Journal of Information Security and Applications, 2023, 74: 103452.

[21] 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. 2021: 76-88.

[22] MAO C, GOLAB W. Sharding Techniques in the Era of Blockchain[C]// 2021 40th International Symposium on Reliable Distributed Systems (SRDS). 2021: 343-344.

[23] CHA K J. Research on blockchain sharding strategy and its application in traditional Chinese medicine data query[D]. Nanjing: Nanjing University of Chinese Medicine, 2022.

[24] ZHANG P, GUO W, LIU Z, et al. Optimized Blockchain Sharding Model Based on Node Trust and Allocation[J]. IEEE Transactions on Network and Service Management, 2023, 20(3): 2804-2816.

[25] ZHANG M, LI J, CHEN Z, et al. CycLedger: A Scalable and Secure Parallel Protocol for Distributed Ledger via Sharding[C]// 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS). IEEE, 2020: 358-367.

[26] RANA R, KANNAN S, TSE D, et al. Free2Shard: Adversary-

resistant Distributed Resource Allocation for Blockchains[J]. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2022, 6(1): 11: 1-11: 38.

[27] YUN J, GOH Y, CHUNG J M. Trust-based shard distribution scheme for fault-tolerant shard blockchain networks[J]. IEEE Access, 2019, 7: 135164-135175.

[28] TIAN J, XU H, TIAN J. SLChain: A secure and low-storage pressure sharding blockchain[J]. Concurrency and Computation: Practice and Experience, 2024, 36(3): e7918. 1-e7918. 15.

[29] LADOSZ P, WENG L, KIM M, et al. Exploration in deep reinforcement learning: A survey[J]. Information Fusion, 2022, 85: 1-22.

[30] ZHANG J, HONG Z, QIU X, et al. SkyChain: A Deep Reinforcement Learning-Empowered Dynamic Blockchain Sharding System[C]// Proceedings of the 49th International Conference on Parallel Processing. New York, NY, USA: Association for Computing Machinery, 2020: 1-11.

[31] LIN Y, GAO Z, DU H, et al. DRL-based adaptive sharding for blockchain-based federated learning[J]. IEEE Transactions on Communications, 2023, 41(11): 3504-3516.

[32] YUN J, GOH Y, CHUNG J M. DQN-Based Optimization Framework for Secure Sharded Blockchain Systems[J]. IEEE Internet of Things Journal, 2021, 8(2): 708-722.

[33] LIU C, WAN J, LI L, et al. Throughput Optimization for Blockchain System with Dynamic Sharding[J]. Electronics, 2023, 12(24): 4915.

[34] WANG J D, LI Q. Improved practical Byzantine fault tolerance consensus algorithm based on Raft algorithm[J]. Journal of Computer Applications, 2023, 43(1): 122-129.

[35] BAI S Z, CHEN M J. Research on Layering and Sharding of Blockchain for Industrial Internet[J]. Computer Engineering, 2023, 49(3): 58-66, 79.

[36] LI C, HUANG H, ZHAO Y, et al. Achieving Scalability and Load Balance across Blockchain Shards for State Sharding[C]// 2022 41st International Symposium on Reliable Distributed Systems(SRDS). IEEE, 2022: 284-294.

[37] LI J, NING Y. Blockchain Transaction Sharding Algorithm based on Account-Weighted Graph[J]. IEEE Access, 2024, 12: 24672-24684.

[38] CAI X, GENG S, ZHANG J, et al. A Sharding Scheme-Based Many-Objective Optimization Algorithm for Enhancing Security in Blockchain-Enabled Industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7650-7658.

[39] HONG Z, GUO S, LI P. Scaling Blockchain via Layered Sharding[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3575-3588.

[40] HUANG H, PENG X, ZHAN J, et al. BrokerChain: A Cross-Shard Blockchain Protocol for Account/Balance-based State Sharding[C]// IEEE INFOCOM 2022 — IEEE Conference on Computer Communications. 2022: 1968-1977.

[41] SET S K, PARK G S. Service-Aware Dynamic Sharding Approach for Scalable Blockchain[J]. IEEE Transactions on Services Computing, 2023, 16(4): 2954-2969.

[42] MU K, WEI X. EfShard: Toward Efficient State Sharding Blockchain via Flexible and Timely State Allocation[J]. IEEE Transactions on Network and Service Management, 2023, 20(3): 2817-2829.

[43] ZHANG Y, PAN S, YU J. TxAllo: Dynamic Transaction Allocation in Sharded Blockchain Systems[C]// 2023 IEEE 39th International Conference on Data Engineering (ICDE). 2023: 721-733.

[44] MIZRAHI A, ROTTENSTREICH O. State Sharding with Space-aware Representations[C]// 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). 2020: 1-9.

[45] TENNAKOON D, GRAMOLI V. Dynamic Blockchain Sharding[C]// 5th International Symposium on Foundations and Applications of Blockchain 2022(FAB 2022). Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2022.

[46] ZHENG P, XU Q, ZHENG Z, et al. Meepo: Sharded Consortium Blockchain[C]// 2021 IEEE 37th International Conference on Data Engineering(ICDE). 2021: 1847-1852.

[47] LIU Y, LIU J, LI D, et al. FleetChain: A Secure Scalable and Responsive Blockchain Achieving Optimal Sharding[C]// QIU M. Algorithms and Architectures for Parallel Processing. Cham: Springer International Publishing, 2020: 409-425.

[48] FATHI F, BAGHANI M, BAYAT M. Light-PerIChain: Using lightweight scalable blockchain based on node performance and improved consensus algorithm in IoT systems[J]. Computer Communications, 2024, 213: 246-259.

[49] WANG Y, WANG W, ZENG Y, et al. Grading Shard : A new sharding protocol to improve blockchain throughput[J]. Peer-to-Peer Networking and Applications, 2023, 16(3): 1327-1339.

[50] LI M, WANG W, ZHANG J. LB-Chain: Load-Balanced and Low-Latency Blockchain Sharding via Account Migration[J]. IEEE Transactions on Parallel & Distributed Systems, 2023, 34(10): 2797-2810.

[51] XU J, MING Y, WU Z, et al. X-Shard: Optimistic Cross-Shard Transaction Processing for Sharding-Based Blockchains[J]. IEEE Transactions on Parallel & Distributed Systems, 2024, 35(4): 548-559.

[52] JIA L, LIU Y, WANG K, et al. Estuary: A Low Cross-Shard Blockchain Sharding Protocol Based on State Splitting[J]. IEEE Transactions on Parallel & Distributed Systems, 2024, 35(3): 405-420.

[53] WANG Y, LI J, LIU W, et al. Efficient Concurrent Execution of Smart Contracts in Blockchain Sharding[J]. Security and Communication Networks, 2021, 2021: e6688168.

TAN Pengliu, born in 1975, Ph.D, associate professor, is a member of CCF (No. 19252M). His main research interests include blockchain, cyber-physical system, intelligent medical care, intelligent transportation system, etc.

(责任编辑:柯颖)