·区块链理论与技术· 文章编号：1000-3428(2022)06-0001-10 文献标志码：A 中图分类号：TP391

区块链分片技术综述

黄华威[1]，孔 伟[2]，彭肖文[1]，郑子彬[1]

（1.中山大学 计算机学院，广州 510000；2.武汉理工大学 航运学院，武汉 430000）

摘 要：区块链作为分布式账本的关键技术之一，其去中心化、可匿名、不可篡改的特性受到学术界和工业界的青睐，被广泛应用于金融、数字货币、公共服务等领域。分片技术作为区块链扩容的主流方式之一，能够在不降低区块链去中心化程度的同时实现高性能的链上扩容，从而解决区块链可拓展性不足以及吞吐量较低的问题。介绍近年来出现的分片技术以及相关协议，总结分片技术的关键理论与方法，从分片配置、重配置、片内共识协议、跨片共识协议、状态存储等方面对分片技术方案进行对比，归纳不同分片方案在网络分片、交易分片、状态分片等设计中存在的优势和不足。同时，阐述一些经典分片技术在性能和实现方式上的特点，对许可区块链和无许可区块链、片内共识协议、跨片共识协议、准入性方案、状态分片方式等进行分析和概述。在此基础上，从分片内、分片间以及系统层级的角度总结分片技术当前所面临的困境和挑战，并对该领域的发展前景及未来研究方向加以展望。

关键词：区块链；分片技术；共识机制；分布式账本；可扩展性

开放科学（资源服务）标志码（OSID）：

中文引用格式：黄华威，孔伟，彭肖文，等.区块链分片技术综述[J].计算机工程，2022，48(6)：1-10.

英文引用格式：HUANG H W，KONG W，PENG X W，et al.Survey on blockchain sharding technology[J].Computer Engineering，2022，48(6)：1-10.

Survey on Blockchain Sharding Technology

HUANG Huawei[1]，KONG Wei[2]，PENG Xiaowen[1]，ZHENG Zibin[1]

（1.School of Computer Science and Engineering，Sun Yat-Sen University，Guangzhou 510000，China；
2.School of Navigation，Wuhan University of Technology，Wuhan 430000，China）

【Abstract】As one of the key technologies of distributed ledger，blockchain is favored by academia and industry for its decentralized，anonymous，and tamper-proof characteristics.It is widely used in finance，digital currency，public services，and other fields.As one of the mainstream methods of blockchain，sharding technology can realize high-performance capacity expansion on the chain without reducing the degree of decentralization of the blockchain，to address problems of insufficient scalability and low throughput. This study introduces the sharding technology and related protocols of recent years，summarizing the key theories and methods of sharding，comparing the sharding technology schemes in terms of of sharding configuration，reconfiguration，intrachip consensus protocol，cross-chip consensus protocol，and state storage.The advantages and disadvantages of different sharding schemes are further summarized with respect to the design of the network，transaction，and sharding state. The characteristics of some classical fragmentation technologies are expounded upon in terms of performance and implementation mode，analyzing and summarizing licensed blockchain and unlicensed blockchain on-chip consensus protocol，cross-chip consensus protocol，access scheme，state fragmentation mode，and the like.On this basis，the current difficulties and challenges of sharding technology are presented from the perspective of system level intra-sharding and inter-sharding，suggesting future development prospects and research directions in this field.

【Key words】blockchain；sharding technology；consensus mechanism；distributed ledger；scalability

DOI：10. 19678/j. issn. 1000-3428. 0063887

0 概述

2016年，LUU等[1]提出一种Elastico算法，其将数据库中扩容的分片方式[2-4]与区块链技术相结合，自此之后，关于区块链分片技术的研究一直层出不穷，不少学者从分布式账本、共识机制、分片方式等方面针对分片技术进行了大量研究。

区块链主要包括网络分片、交易分片、状态分片3种分片方式，其中，网络分片是基础，状态分片是瓶颈。网络分片通过一定的组织方式将整个网络分成

基金项目：国家重点研发计划(2020YFB1006005)；国家自然科学基金(61902445，62032025)；广东省自然科学基金面上项目(2019A1515011798)；广州市基础研究计划-基础与应用基础研究项目(202102020613)。

作者简介：黄华威(1988—)，男，副教授、博士、博士生导师，主研方向为区块链技术；孔 伟、彭肖文，硕士研究生；郑子彬，教授、博士、博士生导师。

收稿日期：2022-02-04 **修回日期：**2022-04-08 **E-mail：**huanghw28@mail.sysu.edu.cn

不同分片，各个分片并行处理整个区块链中的部分交易，各部分交易完全不同，从而同时完成多笔交易验证。交易分片使得各个网络分片对交易具有更强的处理能力，其将客户端的跨片交易分成若干个相关的子交易，不同分片的跨片交易可以并行处理。为了降低各个节点存储账本的压力，状态分片将各部分完全不同的账本分别存储在各个分片（分片内的节点往往存储同一版本的账本），整个分片网络组成一个完整的账本。在现行的技术条件下，网络分片和交易分片都具有比较理想的实现方式，而实现状态分片还存在很多技术问题，状态分片制约着分片技术的发展。

分片技术虽然在一定程度上有效解决了区块链的可扩展性问题[5]，但还存在一定的不足需要改进：整个分片机制在运行过程中有大量时间用于处理交易以外的工作，同时，为了防止节点作恶，不少分片技术需要大量时间和开销进行分片重配置[6]，如何提升分片机制运行过程中用于交易处理的有效时间比率是一个需要解决的问题[7]；状态分片是分片方式中极难实现的一环，在状态分片情境下，跨片交易的验证过程变得极为困难，不同的分片节点存储的账本不同，需要通过一定的方式进行交易转移或账本状态交流[8]，因此，更加有效地实现数据迁移同时减轻各个节点的负担，也是区块链分片技术面临的挑战；分片区块链的安全性也应得到研究人员的关注，更小规模的分片意味对双花攻击防御能力的下降，安全性更高的片内共识协议也将付出更高的共识代价，大多数协议对于安全性的分析集中在拜占庭对手规模、信息可靠性以及分片随机性方面，而对于区块链系统整体的安全性则考虑不充分，对于传统区块链中存在的攻击方式、分片区块链中独有的攻击方式，以及许多分片区块链协议难以抵御网络层面的攻击，这些问题都将成为研究人员关注的焦点。

本文介绍区块链分片技术的研究进展，对分片技术的一般实现步骤进行总结，通过对当前技术的对比剖析归纳分片技术所面临的挑战，同时对该领域未来的发展方向进行展望，以期为区块链分片技术的进一步研究提供理论参考。

1 背景介绍

1.1 区块链技术面临的挑战

区块链技术起源于中本聪于2008年提出的比特币系统[9]，在比特币的信任模型中，用户之间的信任源于对整个系统的信任，只要整个系统的安全假设被满足，这种信任就可以持续。为了实现这种信任模型，整个区块链所有的交易需要各个节点进行验证和存储，从而浪费了大量的时间和空间，也导致区块链系统存在低吞吐、高延迟的瓶颈，出现严重的可扩展性问题。区块链技术现存的一些突出问题总结如下：

1）交易吞吐量低。为了确保区块链的交易不可篡改，比特币的平均吞吐量为7笔/s[10]，以太坊[11]的平均吞吐量为30笔/s，而现行的大型中心化交易处理场所（如Visa）每秒的交易确认数可达上千[12]。为了处理数量庞大的用户交易，提升区块链的交易吞吐量十分重要。

2）交易延迟高。在比特币中，为了确保高安全性，各个节点之间需要频繁地广播交互，额外的通信开销使得比特币的交易延迟增大，比特币的出块速度一般为10 min/块。因此，在忽略网络因素的情况下，通过减少交易过程中的开销从而降低交易延迟也是区块链的优化目标。

3）可扩展性低。随着节点数目的增多以及账本容量的增大，提升区块链可扩展性以及优化账本存储方式、提升存储效率[13]也是亟待解决的问题。

1.2 常见区块链扩容技术

为了提升区块链的可拓展性，近年来，研究人员提出了多种区块链扩容方案。总体而言，常见的区块链扩容方案分为Layer0、Layer1、Layer2这3层技术[14]。其中：Layer0层主要针对数据传播方式进行改进；Layer1层通过共识协议、P2P网络[15]、数据结构等链上技术实现区块链性能提升，其包括分片技术、Bitcoin-NG、DAG分布式账本等；Layer2层大多为非链上技术，如状态通道。

1.2.1 分片技术

分片技术能够克服区块链所面临的可拓展性问题，作为一种链上扩容方式，其能在不牺牲中心化程度的同时提高区块链的性能，因此，分片技术逐渐成为区块链扩容的主流方法之一。分片技术将整个区块链网络分成不同分片，由各分片的节点负责处理所在分片的事务以及存储分片的状态[16]，通过并行验证事务，整个区块链的吞吐量近似线性地提升。同时，随着节点数目的增加，整个网络的分片数量也增多，全网的事务处理能力进一步提高。分片技术一般分为定义分片配置、片内和跨片共识协议、重配置等阶段，从而构成一个完整的分片区块链系统。

1.2.2 状态通道

状态通道[17]在区块链主链下开展新的状态通道供大多数交易离线使用[18]，其将区块链作为仲裁平台。所有需要进行交易的网络用户将一定数量的资金存在链上，同时会与另一个用户开启状态通道，并将这笔资金作为交易的抵押品。状态通道间接地提升了系统的交易吞吐量，其最大的优势是交易几乎可以在一瞬间完成，其中的交易不会阻塞主链，但是额外创建状态通道并不会提高区块链的可扩展性。同时，状态通道容易受到DoS攻击[19]。由于状态通道是在Layer2层进行的扩容技术，因此其与Layer1层的分片技术可以同时使用[20]。

1.2.3 Bitcoin-NG

Bitcoin-NG[21]将原先比特币验证和出块的机制进行分离,能够在一定时间内创建更多的块,从而提升整个区块链的交易处理能力。在记账人选取阶段,Bitcoin-NG仍然采用原先的PoW算法[22],由全网竞争记账权,在交易记账阶段由记账人进行交易打包和全网广播。但是,Bitcoin-NG对去中心化要求做了一定折中,记账人在进行交易打包和全网广播时所实施的不良行为,会使得整个系统面临一定风险[23]。

1.2.4 DAG分布式账本

DAG分布式账本[24]主要对区块链状态存储进行改进,每个交易单元或包含交易的区块单元能够同时被多个新加入的节点引用,多个节点可以同时向账本中新增交易或区块单元,因此,DAG分布式账本可以支持各种实际场景下的高并发需求,具有更好的可扩展性。与DAG分布式账本相比,分片技术更加倾向于改进交易的验证方式,因此,两者可以结合使用。

1.3 许可区块链和无许可区块链中的分片技术

许可区块链(Permissioned Blockchain)[25]由具有一定程度信任并已知、已识别的参与者操作,采用更加传统的共识协议,这种协议不需要成本高昂的挖掘过程,同时在对手规模和容错率的设定上也更加灵活。许可区块链在进行分片[26]后,通常不需要重新配置(Reconfiguration)环节,分片中的记账权往往在少数确定的节点中,因此,节点的安全性较高[27]。在AHL[28]中,采用TEE[29]的硬件来保证可信的执行环境,在此基础上,提出应用于许可区块链的协议,该协议可以灵活地根据拜占庭节点和非拜占庭节点进行调控,从而满足一定的安全性要求。Sharper[30]同样也是应用于许可区块链的协议,其采用分片结合DAG分布式账本的结构,每个分片保存一份账本,在许可区块链中不需要挖矿环节,因此,每笔交易可作为一个块,片内事务由片内单独成块上链,跨片交易由相关分片共同维护。

无许可区块链(Permissionless Blockchain)由于信任度较低(甚至不存在任何信任),因此通常采用挖矿机制,通过PoW来验证交易。具有代表性的无许可区块链协议包括Elastico、OmniLedger[31]、RapidChain[32]等,在这类协议中,节点加入分片需要通过解决PoW问题来验证身份,交易在验证后也需要一定的数据结构进行打包。Monoxide[33]是无许可区块链中较前沿的技术,研究人员认为该技术同时满足了安全、性能、去中心化3个需求[34],连弩挖矿(Chu-ko-nu Mining)能够在一段时间内出多个块,同时通过多个其他分片来对多个块进行验证,即使全网都进行了分片,恶意节点仍然需要与全网算力进行对抗,从而保证了Monoxide的安全性和去中心化。

2 分片技术的关键理论与方法概述

随着数据库的逐渐扩容,为了简化各个节点的存储空间,数据库开始采用分片技术来提高数据的存储效率[35]。区块链和数据库本身存在一些不同因素,区块链分片技术不仅要保持对各分片中存储账本的维护,更要有利于区块链上动态交易的验证。因此,将分片技术引入到区块链中,不仅需要将区块链上的各种属性(网络、交易、状态)进行分片,同时也要考虑区块链本身复杂的数据结构和存储形式[36]。

2.1 分片配置

在区块链分片技术中,首先要实现网络分片,网络分片通常要考虑分片规模、分片安全性、分片方式等因素,分片过程通常使用随机函数来实现。

2.1.1 Elastico

Elastico[1]使用epochRandomness函数进行计算,每个节点都有自己的IP、PK(公钥),结合随机数epochRandomness计算出满足下式条件的nonce:

$$O=\mathrm{H}(\mathrm{epochRandomness}||\mathrm{IP}||\mathrm{PK}||\mathrm{nonce})\leqslant 2^{\gamma-D}$$

其中:D为预定义的网络节点解决PoW问题的工作量大小参数;γ为预定义的H函数的输出位数。

每个节点根据自己的O值确定分片位置,分片中的各个节点为了确认彼此,需要进行广播。

2.1.2 RapidChain

RapidChain[32]的分片配置只进行一次(即原文中的Bootstrap环节),之后不断地进行共识和重配置。在分片配置环节,整个网络持续地从低一层的节点中构造sampler graph以形成一个随机二分图[37],在所有节点完成计算后,将每个group内哈希值最小的节点选为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root group。root group负责选择参考委员会(Reference Committee)成员,参考委员会完成所有节点的随机划分分片。

通过以上2种分配方式可以看出,在协议的开始阶段对节点进行分片的过程,需要各个节点进行自身分片位置计算以及在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。分片函数的设计往往以节点身份(IP、PK、Hash)[38]作为参数。

2.2 分片重配置

为了保证各个分片的安全性并防止节点之间作恶行为发生,在一个分片纪元之后,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,当有新节点加入时,需要对新加入节点进行分配。上述过程通常称为分片重配置(Reconfiguration)[31],分片重配置的方式分为全随机分片和部分随机分片2种。

2.2.1 二次全随机分片

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[39],同时也能将新节点加入分片中。新加入的节点需要解决PoW问题,在解决PoW问题后,节点会得到一个相对应的值(即上文epochRandomness函数中的O),供分片时计算分片位置使用。如果节点错过当前纪元的分片环节,则等待下一个纪元再确定分片位置。解决PoW问题提高了节点加入分片的成本,

但可以有效防止女巫攻击(Sybil Attack)[40]。

Elastico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。

虽然二次全随机分片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交接,在每次的二次全随机分片期间,整个网络都要为分片重新进行计算和广播,无论在开销还是时间上,都大幅降低了整个区块链的性能。因此,文献[41]提出MVCom方案,其对Elastico协议的分片重配置设计进行优化,通过设计分布式算法[42],为每一轮若干个区块链分片选取出最有价值的部分委员会,同时支持处理分片委员会的动态加入和离开,该机制可以在分片区块链的交易吞吐量与分片内交易等待时延之间找到一种平衡。

2.2.2 部分重分配

在保证整个区块链系统网络安全的前提下,将部分分片节点随机进行重分配,既能保证区块链系统的安全性,又可以降低开销,减少重配置过程的等待时间。

研究人员在RapidChain中设计有限布谷鸟原则(Bounded Cuckoo rule)[43],在每个epoch中都通过参考委员会将其他委员会分为2类,分别是活跃成员占大多数的活跃委员会和不活跃成员占大多数的消极委员会。当有新节点加入时,参考委员会会将新节点随机加到某个活跃委员会中,并把该委员会中的固定数量节点随机加入到不同的消极委员会中,既实现了对新节点的分片处理,又调控了消极委员会和积极委员会之间的活跃节点数量,间接提高了整个区块链的分片活跃度。

在进行重配置的过程中,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。

2.2.3 自由选择重分配

SSChain[44]在分片重配置上充分考虑用户需求,当有新节点加入时,新节点可以根据增益函数GPH(BR=BlockReward,HP=HashPower,BI=BlockInterval)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函数综合考量分片出块收益、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(即对于算力的宏观分配),又充分考虑到用户的个人意愿。CPH函数计算如下:

$$\frac{\mathrm{BR(root)}}{\mathrm{BR(shard)}}=\frac{\mathrm{HP(root)*BI(root)}}{\mathrm{HP(shard)*BI(shard)}}$$

$$\mathrm{GPH}=\frac{\mathrm{BR}}{\mathrm{BI}}\Big/\mathrm{PresentHP}$$

相较前2种重分配方式,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,但是其对于恶意行为的抵御能力低于区块链系统调控下的重配置方案。

2.3 片内共识协议

在完成分片配置后,区块链需要进行交易共识,共识分为片内共识和跨片共识。片内共识要求同一分片内各个节点按照所在分片的协议进行共识和广播,最终得出整个分片的共识结果,片内共识协议主要分为基于PoW的片内共识协议和基于BFT的片内共识协议。

2.3.1 基于PoW的片内共识协议

虽然PoW共识庞大而复杂的计算过程消耗了大量算力,但是其结合一定节点特征的数字运算优势在部分场景中受到人们的青睐。基于PoW的片内共识协议通常在计算过程中以节点身份或所在分片编号为参数进行运算,节点身份标号或所在分片标号具有唯一性,因此,它们可以作为打包块的标识符。

SSChain和Monoxide均采用PoW作为片内共识协议。在Monoxide中,分片在解决一个PoW问题的时间内出不多于剩余其他分片数量的块,然后将多个块交由其他分片进行验证并再次出块,通过2层共识结构确保交易的合理性。如图1所示,Monoxide采用连弩挖矿(Chu-ko-nu Mining),将每个共识组的防御能力提升到51%,每次出块时Hash函数覆盖多个刚要出块的块头进行计算,同时这些块头共用一个nonce,编号b的当前共识组将这m个块头按序排列,构造Merkle树[45],然后通过哈希计算覆盖<MerkleRoot,b,m,nonce>数据结构,在出块时,相关信息会被广播到特定的共识组$i(b\leqslant i<b+m)$,确保其他每个分片只出一个块,因此,即使个别共识组有延迟也不影响其他块的出块。

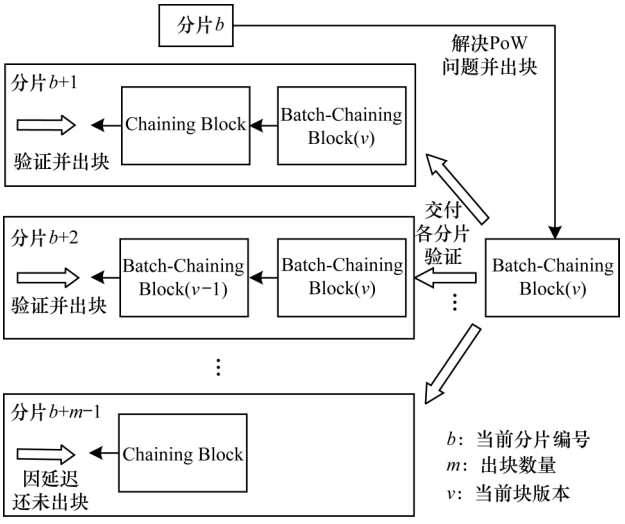

图1 Monoxide的出块方式

Fig.1 Block generation mode of Monoxide

2.3.2 基于BFT的片内共识协议

很多协议的片内共识常会选择使用BFT类型的算法[46],如Elastico采用拜占庭共识协议,OmniLedger采

用基于ByzCoin[47]的改进ByzCoinX，RapidChain采用gossip[48]，Sharper采用PBFT[49]。基于BFT的共识协议通过分片内多个节点验证共识来保证交易的安全性和有效性。

Zilliqa[50]在各个分片内以较高频率运行PBFT共识，PBFT共识具有最终交易性、能耗低等优点。传统PBFT共识中的主要环节包括pre-prepare、prepare、commit这3个阶段，prepare与commit这2个阶段的通信复杂度为$O(n^2)$。Zilliqa采用两轮的EC-SChnorr多重签名[51]来代替传统PBFT共识中的prepare和commit阶段，从而将PBFT共识的通信复杂度降为$O(n)$，其共识流程如图2所示。

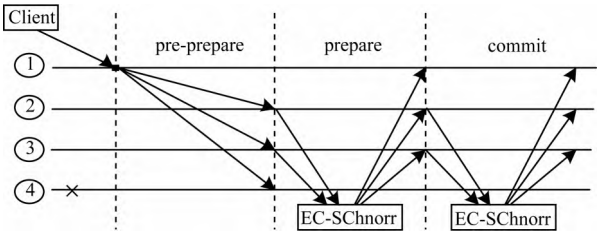

图2　Zilliqa片内共识流程

Fig.2　Zilliqa intra chip consensus procedure

2.4　跨片共识协议

在片内共识时，片内各个节点经过彼此间的广播可直接进行交流。在跨片共识时，由于所存储的信息不相交，不同分片之间各个节点在交易验证过程中需要交流账本状态，因此跨片交流的基本单位是各个分片，不同分片执行共同的跨片协议以实现共识。跨片共识的主要方式包括交易原子化、交易集中化和采用类路由协议。

2.4.1　交易原子化

交易原子化是一种跨片交易处理方式，将原交易分解成最小的子交易，在不同分片之间传递子交易。子交易一般为对某个分片的输入交易或对某个分片的输出交易。通过交易原子化处理，一笔跨分片交易可以视作若干笔客户端参与下的片内交易。

OmniLedger提出Atomix协议对跨片交易进行处理，当客户端发起一笔跨片交易时，分解后的子交易经过不同的分片进行验证，当得到交易接受通知时，客户端再发起一笔附上接受凭证的资金解锁请求到需要输出交易的分片，从而完成交易；如果有交易在分片中验证失败，则客户端向其他验证成功的分片发送丢弃交易请求并将锁住的资金退还。OmniLedger的做法虽然在理论上可以实现由不同分片验证交易和不同分片输出交易的目标，但是当客户端不发送资金解锁请求或交易废弃请求时，就会存在资金锁住的情况，当有恶意节点进行大量低额度的交易提交时，也会在各分片间造成极大压力[52]。

2.4.2　交易集中化

交易集中化是指将跨片交易集中到指定链上或指定节点进行统一处理，指定链上或节点上存储了跨片交易所需的全部账本数据，既能对跨片交易进行验证，又能降低跨片交易传播的难度。

在Ethereum 2.0[53]的结构设计中，信标链（Beacon Chain）作为该架构的核心，负责连接主链以及管理各个分片。信标链是Ethereum原链的一条侧链，运行Casper FFG共识。信标链可以验证Ethereum 2.0中的跨分片交易是否发生双花，并且给各个分片提供最终确定性。当系统中跨分片交易数量过多时，信标链本身的局限性可能会成为跨分片交易的性能瓶颈。当前Ethereum 2.0仍未到达部署分片的阶段，因此，信标链结合分片链来处理跨片交易的方式存在广阔的发展空间。

2.4.3　交易类路由协议

RapidChain提出的委员会间路由协议（Inter-committee Routing Protocol）以及Sharper、AHL，都考虑到将跨片交易直接在不同分片之间进行路由处理的相似设计，本文将此类跨片协议称为“类路由协议”。类路由协议指将交易在不同分片之间进行路由传播，而非直接对交易进行分解。

RapidChain对需要进行跨片处理的交易，由分片中的任意节点根据路由表进行路由，路由表中存储$\log_a n$个最近委员会中$\log_a \log_a n$的节点数据[54]，路由通道只要建立后就可以多次使用，例如，需要将交易从分片A路由到分片C，而A到B、B到C之间存在通道，则可以通过$A\rightarrow B\rightarrow C$的路由通道将交易$a$路由成分片$C$的交易$a'$，从而将跨片交易转化为片内交易。

2.5　状态存储

状态分片将整个网络的账本状态分片存储，各个分片维护一部分账本数据，能够有效减少区块链网络节点的存储负担。然而，各个分片的数据不相交不仅会导致跨片交易的验证极为困难，节点在不同分片之间进行重配置时需要进行大量的数据交接，也会降低账本数据的安全性。因此，有研究人员提出对账本存储进行部分分片的方案，相较比特币设计，该方案能降低数据冗余，较好地处理跨分片交易，具有更高的灵活性和实用性。

2.5.1　全分片存储

在全分片存储模型中，整个区块链账本被分成若干份互不相交的账本存储在分片节点中，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。

OmniLedger是典型的全分片协作式账本，各个分片存储完全不同的数据，这样就将交易验证过程

中数据的交流交给跨片共识协议完成,同时在重配置过程中节点也需要对不同分片间的数据进行交接。当选择在每一个epoch后进行分片内节点更新的方案时,必然会有新加入分片的节点,而节点的账本更新会造成数据迁移。有些协议通过设置state block的方式来简化数据迁移过程,当每一个epoch结束后,设置一个state block对之前的块进行总结并且由整个分片进行验算以确认该块正确无误,新加入节点可以从state block开始直接对新交易进行验证。

状态分片中账户状态划分策略不合理将导致各个分片的交易负载不均衡以及跨分片交易比例过高的问题,为此,BrokerChain[55]提出一种新的分片架构,以实现对分片状态的动态划分和调整。该分片协议根据一定时间内的历史交易信息构建一个账户交易状态图,并对其进行划分[56],从而对存储在各分片的账户状态实现动态调整与重新配置。账户状态动态调整策略可以在减少跨分片交易比例的同时实现分片间的负载均衡。

考虑到基于分片机制的区块链可能存在交易分片不均衡[57]的情况,为此,文献[58]研究分片联盟链的云端资源分配对区块链吞吐量的影响,其基于随机优化理论框架,设计针对分片联盟链的资源分配算法,该算法可在一定程度上缓解区块链交易分布不均衡的问题。

2.5.2 半分片存储

Sharper是许可区块链下的分片协议,其将整个账本存储成DAG分布式账本,当存在跨片交易时,由不同分片共同创建状态账本并存储,因此,同一份跨片交易在不同的分片中都需要进行存储,跨片交易在所有参与的相关分片中都存在数据冗余。

洪梓聪等[59]提出一种层级分片的区块链系统Pyramid,该系统允许某些分片(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,桥接分片可以对跨片交易直接验证并进行CoSi[60]共识,将其打包为包含跨片账本数据的跨分片区块,从而提升区块链系统的事务吞吐量,降低事务确认延迟。BrokerChain[55]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。

3 分片技术的现有方案分析

3.1 现有方案对比

近年来,分片技术不断更新迭代,在吞吐量、时延、共识协议的方式等方面都得到优化,提升了分片技术的鲁棒性和可实践性。从表1可以看出:无许可区块链仍然是分片技术的主流方式,以比特币为基础的分片技术更加成熟;许可区块链的应用场景较少,但是近年来相关的分片技术仍然有所发展[61],许可区块链将节点可信度交付给TEE硬件[62]实现,可以给予系统更优的拜占庭容错率以及更加灵活的分片和共识方式。

表1 区块链分片技术归纳

Table 1 Summary of blockchain sharding technology

协议属性	Elastico	OmniLedger	RapidChain	AHL	Monoxide	Sharper	SSChain
提出年份	2016	2018	2018	2019	2019	2019	2019
拜占庭容错率	$x/4$	$x/4$	$x/3$	$x/3$	$x/2$	$x/3$	$x/4$
区块链性质	无许可链	无许可链	无许可链	许可链	无许可链	许可链	无许可链
各节点内账本大小	x	x/k	x/k	x/k	x/k	x/k	x/k
TPS	16 blocks [a]	≈10k tx/s [b]	≈7 300 tx/s [c]	≈3 000 tx/s [d]	≈11 700x tx/s [e]	27 000 tx/s [f]	6 449 txW/s [g]
时延	110 s	≈1 s	8.7 s	≈80 s (节点数为79)	13~21 s	240 ms	—
分片方式	epochRandomness函数	RandHound+VRF-based	Committee election	Rnd	First k bit of address	Geogra-phical distance	Market incentive mechanism
片内共识协议	PBFT	ByzCoinX	Synchronous consensus	AHL+	PoW	PBFT	PoW
通信复杂度	$O(n^2)$	$O(n)$	$O(n)$	$O(n)$	—	$O(n^2)$	—
跨片共识方法	—	Atomix	Routing	2PC+2PL	DHT+Relay tx	PBFT	Root-chain
新节点准入方式	PoW	PoW	PoW	—	—	—	—
重配置协议	epochRandomness函数	RandHound+VRF-based	Bounded Cuck-oo rule	Rnd	First k bit of address	—	Market incentive mechanism
账本迁移率	—	$nk \cdot x/k$	$ck \cdot x/k$	$n(k-1)/k$	0	—	0

在表1中,各符号含义如下:

x:区块链规模大小;

n:节点数;

k:分片数;

c:常数($c<n$);

[a]:100个节点/分片,共16个分片;

[b]:72个节点/分片(恶意节点占12.5%),共25个分片;

[c]:250个节点/分片,共4 000个节点;

[d]:36个分片(恶意节点占12.5%),共972个节点;

[e]:36个节点/分片,共2 048个分片;

[f]:4个节点/分片,共5个分片;

[g]:分片链包含900个节点和60个分片,根链上包含900个节点(恶意节点占25%)。

不同协议片内交易和跨片交易设计都有各自的特点,但也呈现出一定的共性:片内共识协议以基于BFT的协议为主,跨片共识协议以交易可靠性为目的。

基于BFT的片内共识协议具有交易最终性和低能耗的优点,但是在安全性方面弱于基于PoW的片内共识协议,因此,部分分片技术将两者相结合,在若干轮BFT类协议后加入PoW协议以提升分片的安全性。跨片共识协议则以交易可靠性为主要目的,对于跨片交易中的交易代价则关注较少。对于跨片交易的处理,虽然已经有一定的实现方案,但是在跨片交易的模型实验中对于复杂交易和交易数量的控制则显得模糊,部分交易只在较简单输入和输出分片的跨片模型下性能较好,有些往往需要将交易分解为若干笔子交易才能完成跨片交易。因此,无论是提升片内共识交易的效率还是优化跨片交易的过程,都是分片技术有待提高的方面。

为了防止女巫攻击[63],Elastico和RapidChain采用通过新节点解决PoW问题的准入性方案,一些许可区块链因为将节点的安全性托付给TEE硬件[64]实现,所以未声明新节点的准入方式,而其他一些无许可区块链对于新节点加入的协议阐述则显得太过简单。

大多数分片技术在实现网络分片和交易分片的设计上已经初具规模,而在状态分片上则显得比较困难。传统的全存储分片技术一致地将区块链账本平均分配在各个分片中,近年来出现的部分存储分片技术考虑到跨片交易中可能出现的数据迁移问题,灵活地将部分账本状态存储或存储在桥接分片中进行处理,或将区块链分片账本进行动态合并分离[65],从而提高了区块链分片账本的利用率。

此外,从表1也可以明显看出,近年来分片技术的吞吐量取得大幅提升。不同技术在验证时所使用的实验设备和方式不尽相同,将吞吐量、时延等数据作为协议性能衡量指标具有可行性,但是不能一味地为了实现高吞吐量、低时延等目标而忽略了分片技术的完整性、安全性和简洁性。

3.2 分片技术面临的挑战

3.2.1 分片内挑战

在区块链网络中,诚实节点与恶意节点的比例要控制在一定范围内,以保证整个网络的安全性。在比特币中,只有当诚实节点的比例占到51%以上,整个区块链才能抵御双花攻击[66]。在分片区块链中,将诚实节点分布到不同的区块链分片中,虽然系统总体的诚实节点数不变,但是各个分片内诚实节点的实际数量减少,相比针对整个区块链网络进行攻击,攻击者对于单分片攻击的规模更小,攻击成本也更低。

BFT类片内共识协议虽然比PoW类共识协议的能耗更低,但在信息交流的过程中表现出效率低下的问题并对信息过度确认,因此,可以通过优化BFT算法来适当简化信息交流与确认过程中对信息的重复使用[67],或者运用一定的数学方法作为对BFT协议的简化[68],从而在一定程度上提升协议效率。

3.2.2 分片间挑战

在分片区块链中,跨片交易的处理可能涉及若干个分片,当攻击者通过较小的攻击成本实现对单个分片的攻击时,所有和该分片相关的跨片交易也会受到影响。在区块链网络中,跨片交易的比例很高,因此,跨片交易的可靠性和效率对区块链系统吞吐量的影响较大。

虽然部分跨片协议有处理跨片交易的能力,但是还是需要客户端参与才能保证跨片交易的有效进行,未充分优化的跨片共识协议增加了客户端的压力。分片技术对轻客户端的支持也十分重要,既要保证在客户端做到状态分片,最小化客户端存储的账本状态,又要尽可能减少客户端在跨片交易验证过程中的操作步骤。

由于节点的存储空间有限,重配置过程中的节点迁移需要进行大量的数据上传和更新,在节点存储空间无限的假设下,节点可以任意存储足够多的账本数据,不需要在迁移过程中进行账本数据更新,节点基本可以持续运作。对于分片区块链而言,制约区块链性能的最主要因素是存储容量。在当前的节点迁移方案中,设置checkpoint是一个较优的方式,即在很大一个epoch后将过往的若干个块化简为一个块,将各个节点的账本大小控制在2 GB左右。但是,如何提高节点重配置阶段迁移数据的利用率仍然需要深入探究。

3.2.3 系统层级挑战

区块链分片规模影响到很多方面,包括分片安全性、共识协议效率、吞吐量等。但是,现行的分片

大小往往受制于协议的安全性保证，如Zilliqa只有在600个节点以上才能保证安全，而对于区块链网络吞吐量和其他因素则难以全面考虑。同时，分片的重配置调节也是一个值得关注的内容，智能化和动态化的重配置阶段需要考虑到分片活跃度、分片容错率、新加入节点数量等因素，而目前的重配置方案仍然是以更加保证安全性的静态场景为出发点，对其他因素的考虑不足。

大多数协议对于安全性的分析通常集中于拜占庭对手规模、信息可靠性以及分片随机性方面，而在整个安全规模上（包括Layer1和Layer2）的考虑则显得有些薄弱。对于当前区块链中的各种攻击方式，如何在新的分片区块链设计过程中考虑这些防御攻击，从而更加完善地分析所关注区块链的安全性，都是今后的研究方向。本文在对各个协议进行汇总分析的过程中，发现只有OmniLedger利用ByzCoinX来应对DoS攻击[69]，对于其他协议是否能够抵抗Layer1层的攻击以及在Layer2层还有哪些共识性问题，都需要建立一个安全性证明框架。

3.3 分片技术未来展望

本文认为区块链分片技术在未来需要在以下方面继续进行研究：

1）提出更加高效的共识协议，这类协议将优化现有网络的分片方式，从交易分片、状态分片角度提出更好的实现方法，使分片技术提升到区块链扩容技术的新高度。

2）将区块链分片技术与其他扩容技术融合创新。分片技术与其他技术在应用层面并不矛盾甚至可以优势互补，将分片技术与其他扩容技术相结合，既有利于发挥其他扩容技术的优势，又能够拓展分片技术的应用空间。

3）提出标准的区块链分片技术协议。随着分片技术的逐步完善，更标准的分片技术安全性协议也会更完善，安全可靠同时具有高性能的分片技术协议将成为分片技术应用于区块链扩容任务的重要基石，近年来，一些学者也正致力于这个方向的研究[70]。

4）开发区块链分片技术的模拟平台。在分片区块链设计的过程中，现行的开源区块链只适用于当前所关注的研究分支。未来可以设计一套完备的区块链分片流程，从分片规模、节点行为、交易设定、网络构建等方面对分片区块链进行模拟验证，便于区块链分片技术的研究开发人员关注分片区块链中的不同模块，进一步促进区块链分片技术的发展。

4 结束语

近年来，区块链分片技术受到学术界和工业界的高度关注，为解决传统区块链在可扩展性上存在瓶颈的问题，许多研究人员提出了不同的分片技术协议。本文介绍分片技术中的一些经典方法和理论，对这些协议进行对比分析，总结当前分片技术面临的困境和挑战。随着区块链分片技术的发展，未来将会出现更加高效的共识协议、更加完善的扩容技术、更加标准的安全性协议以及更好的分片区块链模拟平台，这些成果都将进一步改善基于分片机制的区块链技术生态。

参考文献

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

[2] CORBETT J C, DEAN J, EPSTEIN M, et al. Spanner: Google's globally distributed database[J]. ACM Transactions on Computer Systems, 2013, 31(3): 8.

[3] GLENDENNING L, BESCHASTNIKH I, KRISHNAMURTHY A, et al. Scalable consistency in scatter[C]//Proceedings of the 23rd ACM Symposium on Operating Systems Principles. New York, USA: ACM Press, 2011: 15-28.

[4] DANEZIS G, MEIKLEJOHN S. Centrally banked cryptocurrencies[EB/OL]. [2022-01-05]. http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf.

[5] CROMAN K, DECKER C, EYAL I, et al. On scaling decentralized blockchains[M]. Berlin, Germany: Springer, 2016.

[6] SYTA E, JOVANOVIC P, KOGIAS E K, et al. Scalable bias-resistant distributed randomness[C]//Proceedings of 2017 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2017: 15-22.

[7] ABRAHAM I, MALKHI D, NAYAK K, et al. Solidus: an incentive-compatible cryptocurrency based on permissionless Byzantine consensus[EB/OL]. [2022-01-05]. https://www.cs.umd.edu/~kartik/papers/8_solidus.pdf.

[8] SONNINO A, BANO S, AL-BASSAM M, et al. Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers[C]//Proceedings of 2020 IEEE European Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2020: 134-145.

[9] SQUAREPANTS S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2022-01-05]. https://bitcoin.org/bitcoin.pdf.

[10] Bitcoin Wiki. Scalability[EB/OL]. [2022-01-05]. https://blochchain.info/stats.

[11] CHERNET H F, JILLEDI S K. A next-generation smart contract and decentralized blockchain platform: a case study on ethiopia[EB/OL]. [2022-01-05]. https://www.researchgate.net/publication/348863176_A_Next-Generation_Smart_Contract_and_Decentralized_blockchain_Platform_A_case_study_on_Ethiopia.

[12] Visa. Visa's transcations per second[EB/OL]. [2022-01-05]. https://usa.visa.com/content_library/modal/benefits/accepting/visa.html.

[13] QI X D, ZHANG Z, JIN C Q, et al. BFT-store: storage

partition for permissioned blockchain via erasure coding[C]// Proceedings of 2020 IEEE International Conference on Data Engineering. Washington D. C. ,USA:IEEE Press, 2020:15-26.
[14] 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.
[15] MILOJICIC D S, KALOGERAKI V, LUKOSE R, et al. Peer-to-peer computing[EB/OL]. [2022-01-05]. https://www. hpl. hp. com/techreports/2002/HPL-2002-57R1. pdf.
[16] JIA D Y, XIN J C, WANG Z Q, et al. Optimized data storage method for sharding-based blockchain[J]. IEEE Access, 2021, 9:67890-67900.
[17] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[EB/OL]. [2022-01-05]. https://coinrivet. com/research/papers/the-bitcoin-lightning-network-scalable-off-chain-instant-payments/.
[18] DAS P, ECKEY L, FRASSETTO T, et al. FastKitten: practical smart contracts on bitcoin[C]//Proceedings of the 28th USENIX Security Symposium. San Diego, USA: USENIX Association, 2019:801-818.
[19] ZHANG P Y, ZHOU M C. Security and trust in blockchains: architecture, key technologies, and open issues[J]. IEEE Transactions on Computational Social Systems, 2020, 7(3): 790-801.
[20] Sharding FAQ[EB/OL]. [2022-01-05]. https://github. com/ethereum/wiki/wiki/sharding/faq.
[21] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: a scalable blockchain protocol[C]//Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation. San Diego, USA: USENIX Association, 2016:45-59.
[22] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]//Proceedings of International Cryptology Conference on Advances in Cryptology. Berlin, Germany: Springer, 1993:139-147.
[23] WANG Z Y, LIU J W, ZHANG Z Y, et al. A combined micro-block chain truncation attack on bitcoin-NG[M]. Berlin, Germany: Springer, 2019.
[24] 高政风,郑继来,汤舒扬,等. 基于DAG的分布式账本共识机制研究[J]. 软件学报, 2020, 31(4):1124-1142.
GAO Z F, ZHENG J L, TANG S Y, et al. State-of-the-art survey of consensus mechanisms on DAG-based distributed ledger[J]. Journal of Software, 2020, 31(4):1124-1142. (in Chinese)
[25] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the 13th EuroSys Conference. Washington D. C. ,USA:IEEE Press, 2018:1-15.
[26] ZHENG P L, XU Q Q, ZHENG Z B, et al. Meepo: sharded consortium blockchain[C]//Proceedings of IEEE International Conference on Data Engineering. Washington D. C. ,USA: IEEE Press, 2021:1847-1852.
[27] ESPEL T, KATZ L, ROBIN G. Proposal for protocol on a quorum blockchain with zero knowledge[EB/OL]. [2022-01-05]. https://eprint. iacr. org/2017/1093. pdf.
[28] DANG H, DINH T T A, LOGHIN D, et al. Towards scaling blockchain systems via sharding[C]//Proceedings of 2019 International Conference on Management of Data. Washington D. C. ,USA:IEEE Press, 2019:123-140.
[29] MCKEEN F, ALEXANDROVICH I, BERENZON A, et al. Innovative instructions and software model for isolated execution[EB/OL]. [2022-01-05]. https://dl. acm. org/doi/10. 1145/2487726. 2488368.
[30] AMIRI M J, AGRAWAL D, EL ABBADI A. SharPer: sharding permissioned blockchains over network clusters[C]// Proceedings of 2021 International Conference on Management of Data. New York, USA: ACM Press, 2021:16-23.
[31] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger: a secure, scale-out, decentralized ledger via sharding[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C. ,USA:IEEE Press, 2018: 583-598.
[32] ZAMANI M, MOVAHEDI M, RAYKOVA M. RapidChain: scaling blockchain via full sharding[C]//Proceedings of 2018 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, 2018:931-948.
[33] WANG J, WANG H. Monoxide: scale out blockchains with asynchronous consensus zones[C]//Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation. San Diego, USA: USENIX Association, 2019:95-112.
[34] 袁勇,倪晓春,曾帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11):2011-2022.
YUAN Y, NI X C, ZENG S, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11):2011-2022. (in Chinese)
[35] BAGUI S, NGUYEN L T. Database sharding: to provide fault tolerance and scalability of big data on the cloud[J]. International Journal of Cloud Applications and Computing, 2015, 5(2):36-52.
[36] LI S Z, YU M C, YANG C S, et al. PolyShard: coded sharding achieves linearly scaling efficiency and security simultaneously[C]//Proceedings of IEEE International Symposium on Information Theory. Washington D. C. , USA:IEEE Press, 2020:203-208.
[37] KING V, SAIA J, SANWALANI V, et al. Towards secure and scalable computation in peer-to-peer networks[C]// Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science. Washington D. C. , USA:IEEE Press, 2006:87-98.
[38] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm[J]. International Journal of Information Security, 2001, 1(1):36-63.
[39] BONNEAU J, FELTEN E W, GOLDFEDER S, et al. Why buy when you can rent? Bribery attacks on bitcoin consensus[C]// Proceedings of International Conference on Financial Cryptography and Data Security. Berlin, Germany: Springer, 2016:19-26.
[40] DOUCEUR J R. The sybil attack[EB/OL]. [2022-01-05]. https://nakamotoinstitute. org/static/docs/the-sybil-attack. pdf.
[41] HUANG H W, HUANG Z Y, PENG X W, et al. MVCom: scheduling most valuable committees for the large-scale sharded blockchain[C]//Proceedings of IEEE International

Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2021: 629-639.
[42] FRÉVILLE A. The multidimensional 0-1 knapsack problem: an overview[J]. European Journal of Operational Research, 2004, 155(1): 1-21.
[43] SEN S, FREEDMAN M. Commensal cuckoo: secure group partitioning for large-scale services[J]. ACM SIGOPS Operating Systems Review, 2012, 46(1): 33-39.
[44] 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.
[45] SZYDLO M. Merkle tree traversal in log space and time[J]. Lecture Notes in Computer Science, 2004, 3027: 541-554.
[46] 甘俊, 李强, 陈子豪, 等. 区块链实用拜占庭容错共识算法的改进[J]. 计算机应用, 2019, 39(7): 2148-2155.
GAN J, LI Q, CHEN Z H, et al. Improvement of blockchain practical Byzantine fault tolerance consensus algorithm[J]. Journal of Computer Applications, 2019, 39(7): 2148-2155. (in Chinese)
[47] KOKORIS-KOGIAS E, JOVANOVIC P, GAILLY N, et al. Enhancing bitcoin security and performance with strong consistency via collective signing[EB/OL]. [2022-01-05]. https://www. usenix. org/system/files/conference/usenixsecurity16/sec16_paper_kokoris-kogias. pdf.
[48] KARP R, SCHINDELHAUER C, SHENKER S, et al. Randomized rumor spreading[C]//Proceedings of the 41st Annual Symposium on Foundations of Computer Science. Washington D. C., USA: IEEE Press, 2000: 565-574.
[49] ABRAHAM I, GUETA G, MALKHI D, et al. Revisiting fast practical Byzantine fault tolerance[EB/OL]. [2022-01-05]. https://arxiv. org/abs/1712. 01367.
[50] PLATFORM S B. The Zilliqa project: a secure, scalable blockchain platform [EB/OL]. [2022-01-05]. https://cryptorating. eu/whitepapers/Zilliqa/positionpaper. pdf.
[51] MAXWELL G, POELSTRA A, SEURIN Y, et al. Simple Schnorr multi-signatures with applications to bitcoin[J]. Designs, Codes and Cryptography, 2019, 87(9): 2139-2164.
[52] LIU Y, LIU J, LI D, et al. Fleetchain: a secure scalable and responsive blockchain achieving optimal sharding[C]// Proceedings of International Conference on Algorithms and Architectures for Parallel Processing. Berlin, Germany: Springer, 2020: 409-425.
[53] Ethereum 2. 0 Spec. Ethereum 2. 0 phase 0-the beacon chain, 2020[EB/OL]. [2022-01-05]. https://github. com/ethereum/eth2. 0-specs/blob/dev/specs/phase0/beacon-chain. md.
[54] MAYMOUNKOV P, ERES D M. Kademlia: a peer-to-peer information system based on the XOR metric[EB/OL]. [2022-01-05]. https://www. scs. stanford. edu/~dm/home/papers/kpos. pdf.
[55] HUANG H, PENG X, ZHAN J, et al. BrokerChain: a cross-shard blockchain protocol for account/balance-based state sharding[C]//Proceedings of IEEE International Conference on Computer Communications. Washington D. C., USA: IEEE Press, 2022: 145-156.
[56] KARYPIS G, KUMAR V. A fast and high quality multilevel scheme for partitioning irregular graphs[J]. SIAM Journal on Scientific Computing, 1998, 20(1): 359-392.
[57] NGUYEN L N, NGUYEN T D T, DINH T N, et al. OptChain: optimal transactions placement for scalable blockchain sharding[C]//Proceedings of IEEE International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2019: 525-535.
[58] 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.
[59] HONG Z C, GUO S, LI P, et al. Pyramid: a layered sharding blockchain system[C]//Proceedings of IEEE Conference on Computer Communications. Washington D. C., USA: IEEE Press, 2021: 1-10.
[60] SYTA E, TAMAS I, VISHER D, et al. Keeping authorities "honest or bust" with decentralized witness cosigning[C]// Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2016: 526-545.
[61] YAO W, YE J Y, MURIMI R, et al. A survey on consortium blockchain consensus mechanisms[EB/OL]. [2022-01-05]. https://arxiv. org/abs/2102. 12058.
[62] SABT M, ACHEMLAL M, BOUABDALLAH A. Trusted execution environment: what it is, and what it is not[C]//Proceedings of IEEE Trustcom/BigDataSE/ISPA. Washington D. C., USA: IEEE Press, 2015: 57-64.
[63] ZHANG S J, LEE J H. Double-spending with a sybil attack in the bitcoin decentralized network[J]. IEEE Transactions on Industrial Informatics, 2019, 15(10): 5715-5722.
[64] ZOU D Q, ZHENG W D, LONG J J, et al. Constructing trusted virtual execution environment in P2P grids[J]. Future Generation Computer Systems, 2010, 26(5): 769-775.
[65] ZHANG J T, HONG Z C, QIU X Y, et al. SkyChain: a deep reinforcement learning-empowered dynamic blockchain sharding system[C]//Proceedings of the 49th International Conference on Parallel Processing. Washington D. C., USA: IEEE Press, 2020: 1-11.
[66] ZHENG J, HUANG H W, LI C L, et al. Revisiting double-spending attacks on the bitcoin blockchain: new findings[C]// Proceedings of IEEE/ACM International Symposium on Quality of Service. Washington D. C., USA: IEEE Press, 2021: 1-6.
[67] GOLAN GUETA G, ABRAHAM I, GROSSMAN S, et al. SBFT: a scalable and decentralized trust infrastructure[C]// Proceedings of the 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Washington D. C., USA: IEEE Press, 2019: 568-580.
[68] YIN M F, MALKHI D, REITER M K, et al. HotStuff: BFT consensus with linearity and responsiveness[C]//Proceedings of 2019 ACM Symposium on Principles of Distributed Computing. New York, USA: ACM Press, 2019: 347-356.
[69] SAAD M, COOK V, NGUYEN L, et al. Partitioning attacks on bitcoin: colliding space, time, and logic[C]//Proceedings of IEEE International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2019: 1175-1187.
[70] NGUYEN T, THAI M T. Denial-of-service vulnerability of Hash-based transaction sharding: attacks and countermeasures [EB/OL]. [2022-01-05]. https://arxiv. org/abs/2007. 08600.

编辑 吴云芳