从扩展性角度看区块链

王 锋，张 强，刘 扬†，刘琳琳，路 阳
(河南工业大学 信息科学与工程学院，郑州 450001)

摘 要：区块链集成密码学、分布式共识、P2P 网络和时间戳等技术，可实现数据一致存储、难以窜改和防止抵赖等功能，解决了开放网络中不依赖任何可信第三方的信任问题。去中心化的特性使得区块链具有广阔的应用前景，但随着应用的深入与拓展，扩展性问题已成为挖掘区块链技术潜力的一个关键挑战。区块链本质上仍是分布式系统，基于此，从分布式系统的扩展性角度对区块链的研究工作进行综述，基于链上扩展、链下扩展和跨链扩展三个方面论述了区块链可扩展的思路和方法，总结了近年来的研究成果；通过对现有解决方案的总结分析，探讨了提高区块链可扩展性所面临问题和未来的研究趋势。

关键词：区块链；扩展性；分片；跨链
中图分类号：TP311 doi: 10.19734/j.issn.1001-3695.2023.02.0075

Research progress of blockchain from perspective of scalability

Wang Feng, Zhang Qiang, Liu Yang†, Liu Linlin, Lu Yang
(*College of Information Science & Engineering, Henan University of Technology, Zhengzhou* 450001, *China*)

Abstract: Blockchain integrates cryptography, distributed consensus, P2P networking, and timestamping technologies, which can achieve functions such as consistent data storage, tamper resistance, and non-repudiation, solving the trust issue in open networks that do not rely on any trusted third parties. The decentralized nature of blockchain gives it a broad range of application prospects. However, as the applications become more extensive and profound, the scalability issue has become a key challenge for unlocking the full potential of blockchain technology. Blockchain is essentially still a distributed system. Based on this, this paper reviews the research work on blockchain from the perspective of the scalability of distributed systems. It discusses the ideas and methods for blockchain scalability from three aspects: on-chain scalability, off-chain scalability, and cross-chain scalability, and summarizes the research achievements in recent years. Building on the summary and analysis of existing solutions, this paper explores the challenges faced in improving blockchain scalability and discusses future research trends in this area.

Key words: blockchain; scalabitity; sharding; cross-chain

0 引言

区块链技术起源于中本聪(Namakoto)2008 年发表的《比特币：一种点对点的电子现金系统》一文[1]，是密码学、分布式共识、P2P 网络、时间戳等技术的集成创新。区块链技术能够实现数据一致存储、难以窜改、防止抵赖等功能，也称为分布式账本技术。传统电子系统中发生的交易是以集中的方式进行，需要受信任的第三方参与，难以避免单点故障[2]和高额交易费用[3]等问题；而区块链系统允许不受信任的实体在没有第三方参与的情况下以不受信任的方式进行交互。区块链系统可被认为是一个分布式数据库，记录区块链网络上所有的交易信息。智能合约[4]的出现进一步提高了区块链交易的灵活性，使得其可以应用于复杂的交易应用场景。

区块链技术与传统货币系统相似，同样存在“三元悖论”，即去中心化、安全性和可扩展性三者不可兼得[5]。可扩展性问题是随着区块链中节点和交易数量的增加而出现的。在用户较多的公共区块链(例如比特币和以太坊)中，每个节点都需要存储和执行计算任务来验证每笔交易，公共区块链需要大量的计算能力、高带宽的互联网连接和大量的存储空间。区块链的冗余存储一定程度提高了数据的公开性和透明性，但每个节点都需要同步最新的账本，会出现巨大的存储压力。截至 2022 年末，比特币大小已经超过 350GB[6]，从区块链网络下载完整账本需要很长时间，直接限制了没有足够存储空间的用户加入区块链网络作为全节点。因此，必须在区块链的三个方面找到平衡，并考虑具体区块链应用的要求。

从扩展性角度看，区块链具有不同于传统的分布式系统的一些特征；区块链系统本来是为了解决特定问题而设计的，比特币及之后的一些区块链系统在衡量去中心化、链上数据和资产的安全性以及用户数量的可扩展性之后，在系统性能方面必然会存在瓶颈。为使区块链系统在具体应用中减少可扩展性方面的局限，比特币之后的部分区块链系统进行了体系结构上的创新。本文从可扩展性角度，对区块链技术的研究工作进行总结和分析，讨论主流的可扩展性解决方案及存在的相关问题和挑战，阐述对区块链可扩展性技术所面临挑战的思考，期望对

收稿日期：2023-02-16；**修回日期：**2023-04-11 **基金项目：**河南省重大科技专项(201300210200，201300210100)；河南省高等学校重点科研项目计划基础研究专项(23ZX017)；河南省重点科技攻关项目(232102211082)；2022 年河南省网络密码技术重点实验室研究课题(LNCT2022-A20)

作者简介：王锋(1974-)，男，河南新郑人，副教授，硕导，博士，主要研究方向为区块链、物联网技术；张强(1997-)，男，河南南阳人，硕士研究生，主要研究方向为区块链；刘扬(1978-)，女(通信作者)，河南洛阳人，教授，博导，博士，主要研究方向为区块链、分布式计算(liu_yang@haut.edu.cn)；刘琳琳(1997-)，女，河南焦作人，硕士研究生，主要研究方向为区块链；路阳(1999-)，男，河南商丘人，硕士研究生，主要研究方向为区块链.

区块链可扩展性技术的研究提供帮助和启发。

1　分布式系统的可扩展性

分布式系统的可扩展性是指系统为了应对将来需求的变化而提供的一种能力[7]，当有新的需求出现时，系统不需要或者仅需要少量的更改就可以支持，而无须重构或者重建整个系统。分布式系统设计的核心要求之一就是系统要具有良好的可扩展性，构建分布式系统的目的是为了获取线性的性能增长。比如本文用一台计算机解决了一些问题，当本文增加一台计算机后只需要一半的时间就可以解决这些问题，或者说每分钟可以解决两倍数量的问题，组成的新系统吞吐量翻了一番。提高分布式系统可扩展性的基本方式分为垂直扩展(Vertical Scaling)[8]和水平扩展(Horizontal Scaling)[9]，如图 1 所示。

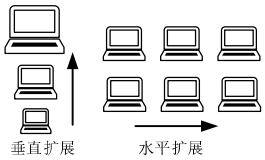

图 1　垂直扩展与水平扩展

Fig. 1　Vertical Scaling and Horizontal Scaling

垂直扩展是指通过提升单机的处理能力从而获得系统的性能提升。垂直扩展又可分为两种方式。

a) 通过增强单机硬件配置而获得系统性能提升。单机硬件性能可以通过增加单机的 CPU 核数，升级性能更好的网卡、硬盘，扩充硬盘容量和系统内存等方式增强。但是，以硬件提升系统的整体性能，效果有限且成本高昂。早期淘宝网的数据库使用的是当时最高端的单机系统(Oracle 数据库+IBM 小型机+EMC 存储)[10]，但随着用户数量的增长，在应对突发的流量激增时仍无法负荷。

b) 通过优化单机软件架构而获得系统性能提升。随着互联网的普及，用户数量呈几何级数增长，系统交互渠道增多，应用程序的逻辑也更为复杂，C10K 问题由此诞生[11]，即单机同时处理 1 万个请求的问题。最初的服务器是基于进程/线程的，如果有新的 TCP(Transmission Control Protocol)连接，就需要分配 1 个进程/线程。如果每个用户都必须与服务器保持 TCP 连接才能进行实时的数据交互，如 Facebook/Tencent 这样的网站同一时间的并发 TCP 连接很可能已经过亿。而进程又是操作系统最昂贵的资源，如果要创建 1 万个进程，单机操作系统是无法承受的，甚至有可能完全瘫痪。C10K 问题的解决为单机性能突破提供了解题思路，即优化软件架构。解决 C10K 问题主要有两种方式[12]，一是对每个连接的处理分配一个独立的进程/线程；二是用同一进程/线程同时处理若干个连接。

但无论是提升单机的硬件性能还是优化系统的架构，这种扩展方式所带来的系统性能提升终究是有限的。面对如 Facebook/Tencent 这样拥有超级用户规模的网站，如果并发 TCP 连接过亿，即便把单机性能发挥到极致，也无法承载如此大的并发访问量。水平扩展通过增加机器(或节点)的数量来提升系统性能的方式因此变得更受人们青睐，成为了目前分布式系统主流的扩展方式，但这种方式通常面临数据一致性和数据耐久性的问题。

a) 一致性问题。一致性是高可用系统的关键指标。如果系统的所有节点在同一时间返回相同的数据，则认为这个系统是一致的。通常来讲，系统的一致性越弱，系统越快，节点获取不到最新数据的可能性也会越高。分布式系统为了确保每个节点都能返回相同的信息，节点之间需要更多的消息通信。但是，在消息通信过程中，有些消息可能会发送失败或丢失，甚至在这个过程中有些节点不可用。

b) 数据耐久性问题。耐久性意味着数据一旦被成功存储就可以持续使用，即使系统中的节点下线，崩溃或数据损坏。不同的分布式数据库数据的耐久性也不同，数据复制是提高耐久性的较为通用的做法，把同一份数据存储在不同的节点上，即使有节点下线，数据仍然可以被访问。

复制(Replication)[13]和分割(Partition)[14]是把数据分布在多台机器节点上的两种常用方式，两者通常一起使用。复制是指把同一份数据复制到位于不同地点的多个不同物理节点上，以冗余的方式进行存储，目的在于降低数据获取延迟，保证数据耐久性，提高数据可用性。分割是指对数据集进行拆分的操作，当数据集很大，单机无法保存或者处理时，通常需要系统对数据集进行拆分，将拆分后的数据子集存放到不同的节点。不同数据库对此操作的定义不同，有分割、分片、区域等，但其含义基本都是相同的。

分布式系统的可扩展性通常可以通过三个方面来看。首先，系统要能在规模上扩展，能够把更多的用户和资源加入到系统中来；其次，如果系统中的用户和资源在地理上相隔遥远，那么这种系统就是地域上可扩展的系统；最后，如果该分布式系统跨越多个独立的管理机构，仍然可以方便地对其进行管理，那么这个系统在管理上也是可扩展的。在解决实际问题时，通常会将垂直扩展和水平扩展有机地结合起来，但由于单机性能总是有极限的，通过增加机器数量的水平扩展，更容易实现，成本也更加低廉。

2　从扩展性角度看区块链

区块链本身是一种分布式系统，区块链网络中交易数量的增加会导致确认时间、网络开销以及延迟和吞吐量的增加。一方面，交易费用与决定交易的确认时间相关，通常更高的费用会有更短的确认时间；另一方面，区块链本身需要保持各个节点数据的一致性，这种一致性是通过共识算法、数据的可靠传输、高冗余存储和密码学技术来实现的[15]。此外，区块链系统中的节点需要同步最新的数据，导致通信和存储的开销越来越大，给区块链中的节点以及系统的整体运行带来巨大的挑战。因此，区块链的可扩展问题已成为挖掘区块链技术潜力的关键问题。

研究人员试图通过链上、链下和跨链三种方式解决这个问题，如图 2 所示。链上方案通过处理区块链内的元素来提高区块链的可扩展性，链下方案通过将链上部分交易移至链下处理从而提高区块链的可扩展性，跨链方案通过打通不同链之间的数据孤岛提高区块链的扩展性。

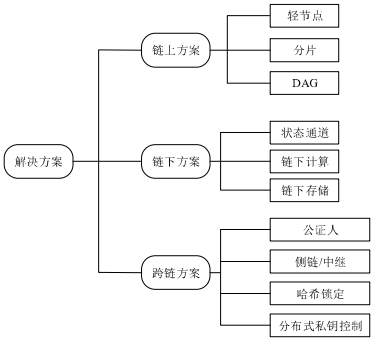

图 2　提高区块链可扩展性方法分类

Fig. 2　Solutions to improve the scalability of blockchain

2.1　链上扩展

链上扩展是指直接修改区块链的规则，改变区块大小、出块时间、共识机制等。比特币 TPS(Transaction Per Second)[16]低的原因是交易确认慢、区块容量小；相应地减少出块时间或增大区块容量以包含更多交易，都能够有效地提高系统的吞吐量。莱特币(LTC)将出块时间减少到比特币的四分之一；比特币现金(BCH)将区块容量提升至 32M，从而提高系统的可扩展性[17]。此外，部分系统采用较为复杂的分片方案和有向无环图(Directed Acyclic Graph, DAG)结构来提高区块链的可扩展性。

2.1.1　轻节点

轻节点是相对于全节点而言的，是运行在小型设备的一种轻量型节点，无须同步完整账本，仅在设备上线时对节点运行环境和输入数据进行验证，需要依靠全节点完成交易验证。而全节点需要消耗自身硬件的算力、电力、网络带宽和存储空间等，同步区块链上的所有交易信息并参与交易数据的验证。全节点在本地保存了一个完整的区块链网络，可进行任何交易的查询和验证，使去中心化成为了可能，同时使得区块链网络更加安全。相对于全节点，轻节点占用的存储空间更小，运行成本更低，因此在很多场景下都比完整节点更为实用。

SPV(Simple Payment Verification Protocol)[18]是首个轻节点协议。如图 3 所示，SPV 轻节点只需要保存所有的区块头数据，依靠全节点可以对交易的有效性进行验证。轻节点的区块头中保存了当前区块中所有交易组成的 Merkle 树的根哈希值；任何一个交易内容的改变，都会使得根哈希值发生变化。轻节点没有同步链上全部数据，不能独立验证交易的有效性，需要依靠全节点和 Merkle 树的特性来验证交易的有效性。

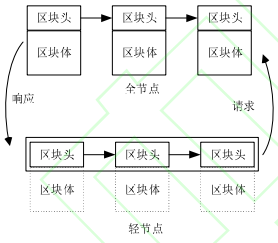

图 3　SPV 轻节点结构示意图

Fig. 3　Schematic diagram of SPV light node structure

轻节点依赖全节点验证交易减弱了区块链去中心化的特性；另一方面，轻节点仍需存储所有区块的块头，这意味着存储开销依然和区块高度成线性关系。因此，许多研究人员对传统轻节点方案进行改进，主要的改进思路有两种：改变验证交易数据的方式和减小块内存储的数据。

1) 改变验证交易数据的方式

Kiayias 等学者[19]提出一种非交互式工作量证明之证明机制(Non-Interactive Proofs of Proof of Work, NiPoPoW)，以提高使用 POW 算法的区块链的性能和扩展其功能。基于 NiPoPoW 的区块链无须验证整条链，只需验证区块链长度的对数个数据，构建证明所需的最长子链，证明某个区块包含该笔交易。与 NiPoPOW 中最长链证明的机制不同，FlyClient[20]采用概率抽样的方法检测作恶节点，先从整条链中随机抽取 k 个区块头，然后在更新的一半子链中再抽样 k 个区块头，如此循环直到剩余的子链长度小于 k，所有抽样出来的区块头集合构成验证集，通过寻找无效的区块头判断节点是否作恶。如图 4 所示，抽样结束后采用 MMR(Merkle Mountain Tree)快速识别区块头的有效性。

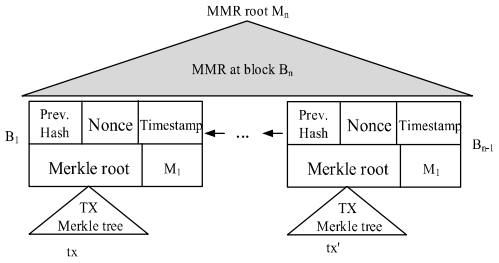

图 4　MMR 树

Fig. 4　Merkle mountain tree

哈希链通过哈希函数 h 生成一串哈希 $S_j(j$ 为自然数且$\geq 0)$。如图 5 所示，链中的每一个元素 S^k 通过前一个元素 S^{k-1} 应用哈希函数 h 计算出来的。Maalla 等学者[21]基于结合布隆过滤器的增量哈希链来验证区块数据，为区块链轻节点提供数据完整性证明。从第一个交易开始增量构建哈希链，直到最后一个交易。假设一个区块包含 L 个交易，T_i 表示索引为 i 的交易，$H(T_i)$代表交易 T_i 的哈希值。为了计算 T_i 希值，需要将该交易与之前的交易(除了第一笔交易)的哈希值串联起来，如式(1)所示。

$$H(T)=\begin{cases}H(T_1);i=1\\ H(H(T_{i-1})\|T_i);1<i\leq L\end{cases} \tag{1}$$

方程的最后一个哈希值是增量哈希链的根，称之为增量哈希根 INR(Incremental Hash Root)，这个值存放在区块头中，并发送给所有节点。节点可以通过再次计算 IHR 来验证区块数据，这个过程可以对区块数据的完整性进行验证；当涉及到验证一个区块中的单个交易时，通过结合增量哈希与布隆过滤器共同实现单个交易的验证。

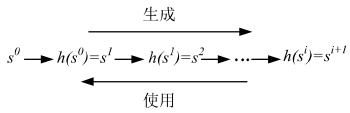

图 5　哈希链

Fig. 5　Hash chain

2) 减小块内存储的数据

Teasung Kim 等学者[22]基于 PBFT(Practical Byzantine Fault Tolerance)共识算法进行改进，提出一种存储压缩共识算法 SCC(Storage Compression Consensus)，降低了加入区块链网络的硬件条件，使得区块链可以在物联网领域有更为广泛的应用。SCC 区块链系统剩余存储容量最小的节点被选为领导者，领导者执行区块链压缩过程并生成压缩块和最新块。验证完成后每个节点将根据自身能力存储块，存储容量受限的节点存储压缩块和最新块并删除所有先前存储的块。每轮共识后，重复此过程。文献[23]提出了一种新的架构 Trail 来提高区块链系统的性能。Trail 的核心是由 TXO(Transaction Output)构建而成的 Merkle 树，称为 TXO 树，其叶子节点存储区块中所有经过验证的 TXO 的哈希值，可以判断一个 TXO 是否被使用。Trail 节点只保存与自己 TXO 相关的 TXO 树的一部分：TXO 树的根哈希值，一个叶子节点的哈希值及其 Merkle 证明。如图 6 所示，TXO 树中粗边框的节点是最右边的叶子节点，灰色节点是最右边叶子节点的 Merkle 证明。通过省略重复的 Merkle 证明减少区块链网络中广播数据的大小，在提高区块链系统的性能同时降低通信和存储的开销。

区块链系统中的轻节点不是越多越好，轻节点只是方便移动设备和物联网设备等轻量级设备使用，部分轻节点需要

依赖全节点提供需要的信息；而全节点的数量则是越多越好，全节点负责交易的广播和验证，从而确保整个系统的稳定运行。表 1 从轻节点的适用范围、验证交易时是否依赖全节点、能否独立验证交易、节点存储大小几个方面对比了上述 6 种典型的轻节点解决方案。经典的 SPV 轻节点方案只需存储全部区块头，需要区块体中数据时需要向全节点请求。改变验证交易数据的方式，不仅可以降低分布式网络传输的开销，也能够降低轻节点对全节点的依赖。NiPoPoW 中节点只需下载和验证重要的区块，从而大大减少同步和验证区块链所需的资源，使得区块链更加轻量级。FlyClient 中轻节点与全节点进行交互，以获取代表整个区块链状态的证明，这个证明只包含区块链中的一小部分，使得轻节点能够更快地验证区块链的状态，并减少对存储和带宽的需求，使其更容易加入区块链网络。减小块内存储数据的方式不仅使得节点能够存储更多的区块数据，也能降低加入区块链网络的要求，使得节点更加轻量化，更适合在资源受限的设备上运行。SCC 将多个交易打包成一个压缩块，能够更有效地利用存储空间，并减少系统存储开销，全节点没有闲置存储空间时，可以简单地删除旧区块，仅存储压缩区块和最新区块；Trail 通过将区块链网络分成若干个区域，每个区域内只需要处理本地的交易和区块，网络中节点只保存与自身相关的一部分数据，从而提高区块链网络的可扩展性。轻节点方案虽然提高了区块链系统的性能，但仍存在一些问题。轻节点只能缓解节点的存储压力，随着交易数量的增加，轻节点需要存储的数据量也随之增加。

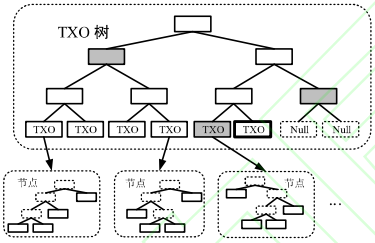

图 6　TXO 树

Fig. 6　TXO tree

表 1　轻节点方案对比

Tab. 1　Comparison of light node solutions

文献	公有链/私有链	是否依赖全节点	能否独立验证交易	节点存储大小
18	公有链	Y	N	全部区块头
19	公有链	Y	Y	部分区块头
20	公有链、私有链	Y	Y	部分区块头
21	公有链	N	Y	全部区块头
22	私有链	Y	N	压缩区块和最新区块
23	公有链	N	Y	压缩后的所有区块头

2.1.2　分片

分片是一种扩展技术，最早应用于数据库扩容，即将一个较大的数据集划分为若干个子集存放在不同的服务器上[24]。区块链的分片技术是一种将整个区块链网络分割成多个小片段，如图 7 所示，每个分片都拥有部分节点，每个分片负责处理交易的一部分，实现了交易的并行化处理，从而提高区块链的交易吞吐量可扩展性。

根据面向对象的不同，分片方式可分为网络分片、交易分片和状态分片[25]。网络分片是指将整个区块链网络分成多个区块链子网络，通常将所有节点随机分配到不同的分片中，分片中的节点只需要处理和验证该分片中的交易和区块，而不需要处理其他分片中的信息。交易分片在网络分片的基础上将整个区块链中的交易分成若干个组，每个组分配到不同的分片中进行处理。交易分片通常采用基于账户或者基于交易的方式进行划分。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，每个分片只处理某些特定账户的交易；基于交易的方式是将所有交易按照其类型或者其他属性进行分类，每个分片只处理某些特定类型或属性的交易。区块链系统中节点为了可以验证交易的有效性，需要存储区块链所有的区块，这种存储方式会给节点造成很大的压力，导致全节点会越来越少，随之，系统的安全性也会越来越差。为了解决这个问题，提出了状态分片这一概念，在网络分片和交易分片的基础上将存储状态也进行分片，每个分片中的节点存储不同的部分，降低节点的存储开销，提高区块链系统的存储可扩展性。

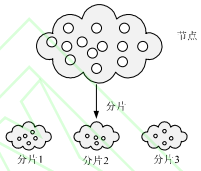

图 7　分片结构示意图

Fig. 7　Fragmentation structure diagram

使用分片技术将区块链网络划分为多个分片，区块链中节点数量可以随着分片数量的增长而增加，实现了交易的并行化处理，提高了区块链的可扩展性，但会牺牲部分的安全性。为了区块链的安全，所有的分片都要容忍节点作恶，在大多数网络中，容忍作恶节点数量的极限是总节点数的三分之一，超出这个限制，无法保证共识过程的安全，即使整个网络中作恶节点的数量低于这个限制，单个分片也是不安全的。如图 8 所示，一个有四分之一作恶节点的网络被平均分为四个分片，而分片 3 中作恶节点数量超过了三分之一，该分片是不安全的，被称为单分片接管攻击。大多数基于分片的区块链协议，使用 PoW 或 PoS 来选举委员，委员会内使用 PBFT 达成共识；另一些则使用特定的共识算法。因此，本文将分片方案分为三类，基于 PoW 和 PBFT 的分片方案、基于 PoS 和 PBFT 的分片方案和基于其他共识算法的分片方案。下面介绍每个分类中具有代表性的分片方案。

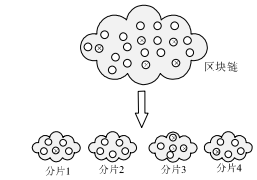

图 8　单分片接管攻击示例

Fig. 8　Example of single fragment takeover attack

1) 基于 PoW 和 PBFT 的分片方案

Elastico[26]是首个基于分片的区块链协议，核心思想是把网络中的节点分成多个小的委员会，每个委员会处理一组单独的交易，实现了交易的并行化处理。Elastico 网络中分片的数量随着网络的规模线性增长，提高了区块链系统的吞吐量，但 Elastico 不支持跨分片通信，无法保证交易的原子性。Elastico 网络采用 PoW 算法选举委员，委员会内部则使用 PBFT 算法进行共识，但委员会重组频繁，同时交易的延迟较高。与 Elastico 一样，OmniLedger[27]使用 PoW+PBFT 的共识方案。此外，OmniLedger 将可验证随机函数(VRF)[28]和 RandHound 协议[29]相结合，避免随机性受到第三方的影响，用于分配成员和选择领导者。OmniLedger 提出了一种基于客户端的跨分片交易协议来确保原子性，从而将通信开销转移

到分片之外。但没有论述 Trust-but-Verify 体系，如何选举 optimistic validators 和 core validators、如何惩罚作恶节点等。

Zamani 等学者[30]提出了一个基于 BFT 的分片协议 RapidChain，在基于 VSS(Verifiable Secret Sharing)[31]的分布式随机生成协议的基础上，引入了一个随机源来消除第三方随机性的限制问题，不牺牲交易效率的前提下能够降低失败概率，避免陷入 BFT 共识算法的困境。同时在不进行委员会重组的情况下可以对多个轮次进行验证，分片内能够容忍 1/2 的作恶节点，总体能够容忍 1/3 的作恶节点。但在出现大量虚假交易时，容易使系统陷入资产不断在分片间转移的循环，可能导致无法进行正常的交易验证。

2) 基于 PoS 和 PBFT 的分片方案

Zilliqa 等学者[32]提出的分片方案允许区块链网络并行处理交易，同时通过压缩通信次数和数据大小降低通信开销，能够极大提升区块链网络的吞吐量。然而，分片中节点需存储全部状态信息，对节点要求较高且没有进行状态分片。Harmony 使用 BLS(Boneh-Lynn-Shacham)签名算法对 PBFT 进行改进[33]，结合 PoS 和改进的 FBFT 算法将通信复杂度由 $O(n^2)$降低到 O(n)，在 Zilliqa 的基础上实现了状态分片，提高了交易并行处理的速度，同时由于分布式随机生成过程，能够确保其分片过程的安全性，但没有详细分析领导者作恶时改进算法的机制和安全性。

3) 基于其他共识算法的分片方案

Sonnino 等学者[34]搭建了一个支持分片的区块链平台 Chainspace，在 PBFT 的基础上提出一种新的分布式原子提交协议(Sharded Byzantine Atomic Commit, S-BAC)用于跨分片的智能合约交易。通过将计算过程和验证过程解耦，降低系统的开销，提高了系统的吞吐量，但没有提供领导者选举的细节和改善分片内部共识冲突的问题。Monoxide[35]针对现有的区块链网络吞吐量低的问题提出了异步共识组区块链网络。将区块链网络划分成为多个独立和并行的区域，高效处理跨越不同区域的交易。提出一种新颖的工作量证明方案 Chu-ko-nu 挖矿，可确保每个区域的有效挖矿能力与整个网络处于同一级别，避免挖矿算力稀释。

表 2 从分片方案的交易模型、采用的共识算法、分片容忍作恶节点数、整体容忍作恶节点数、是否支持跨分片交易、区块链网络同步方式和是否支持智能合约等方面进行分析对比。不同的分片方案目的是相同的，提高区块链系统的可扩展性。通常 UTXO 模型更适合交易分片，账户模型支持智能合约能够实现更复杂的交易；使用不同的共识算法容忍的作恶节点数不同，上述方案只有 Chainspace 是需要许可的区块链。多数分片方案都是基于交易分片的，只有 Harmony 方案实现了状态分片，每个分片中的节点存储不同的部分。在任何分片方案中都要考虑节点的动态变化，为了避免分片是静态的和抵御攻击，网络必须接受新节点并以随机方式将它们分配给不同的分片，即每隔一段时间网络会重新进行划分。基于状态分片的方案，每个分片只维护一部分状态，因此重新划分网络可能会导致整个系统不可用，直到同步完成；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。

分片数量越多，区块链并行化处理交易的数量越多，但也会带来一些问题。一方面，分片数量过多会稀释区块链网络的算力，当单个分片的算力以及验证节点的数量远低于分片之前的整个网络，容易遭受 51%算力攻击。跨分片交易会涉及多个分片，较小的分片遭受攻击时，和遭受攻击分片相关的跨分片交易都会受到影响，分片之间需要克服双花攻击、跨链交易原子性、跨分片交易的 DDoS 攻击等问题。区块链网络中，跨片交易的占比很高，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很大。另一方面，分片数量过多会导致区块链系统花费大量的时间处理与交易无关的事情，如何进行分片、构建委员会和分片重配置等都会带来额外的时间开销和通信开销。

表 2　分片方案对比

Tab. 2　Fragmentation scheme comparison

文献	交易模型	共识算法	分片内容忍作恶节点数	整体容忍作恶节点数	跨分片交易	网络同步方式	智能合约
26	UTXO	PoW+PBFT	1/3	1/4	N	部分同步	N
27	UTXO	PoW+PBFT	1/3	1/4	Y	部分同步	N
30	UTXO	PBFT	1/2	1/3	Y	部分同步	N
32	账户	PBFT	1/3	1/4	Y	异步	Y
33	账户	PoS+FBFT	1/3	1/4	Y	同步	Y
34	Object-driven	BFT	1/3	1/4	Y	异步	Y
35	账户	Zones	1/2	1/2	Y	异步	N

2.1.3　有向无环图

有向无环图(DAG)是一种常用的数据结构，经常被用于解决动态规划、寻求最短路径、数据压缩等问题。图 9 展示了链表、树和有向无环图三个复杂度递进的数据结构。链表是一条带有方向的链；树是有分叉的，但是任意两个节点间只有一条路径能到达另外一点，也就是不存在闭环；而图是可以存在闭环的数据结构。

区块链通常是链式结构，但基于 DAG 的区块链在结构上发生了变化。通常的区块链和基于 DAG 的区块链的结构差异如图 10 所示。链式的区块链是单线程的，而 DAG 结构的区块链是多线程的；链式的区块链所有交易记录都记在同一个区块中，而 DAG 结构的区块链每笔交易被单独记录；链式的区块链组成单元是 Block(区块)，而在 DAG 中，每个交易被视为一个节点，并且每个节点可以有多个父节点和多个子节点。父节点表示此交易的输入，子节点表示此交易的输出，这种数据结构允许数据并行化处理，且不需要等待整个区块被挖掘，从而提高了交易速度和吞吐量。

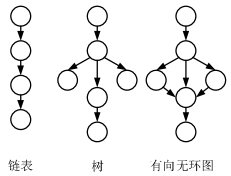

图 9　链表、树和有向无环图

Fig. 9　Linked List, Trees and Directed Acyclic Graph

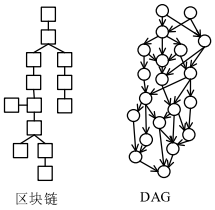

图 10　链式区块链和 DAG 区块链

Fig. 10　Chained Blockchain and DAG Blockchain

基于 DAG 的区块链在结构上发生了变化，根据区块链网络的拓扑结构，可分为平行、收敛和发散三种类型。

1) 平行的网络拓扑结构

平行的网络拓扑结构是指区块链中交易由一组节点以多条链的形式维护。节点分别维护其链/账户，复杂性取决于自身的属性，但需要引入一种额外的排序算法。Hasgraph[36]网络中的每个节点维护一个单独的链，节点在本地创建一个事件用于记录接收的信息，包含时间戳、交易的相关信息和交叉引用的哈希等，节点之间通过 Gossip 协议进行交互。如图 11 所示，Hashgraph 的网络是由节点维护的平行链之间相互引用构建而成的，这些引用指向自身链上的最新事件，也指向该节点收到的另一个节点的最新事件，通过新交易的发生和 Gossip 协议的传输，每个节点都会收到所有的事件。哈希图通过虚拟投票的方式来达成共识，事件最终被认为有效必须经过可见、强可见、决定三个阶段，通过这种方式，事件可以按照全局的总顺序进行排序。

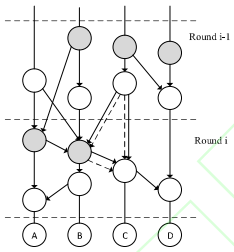

图 11　Hashgraph

Fig. 11　Hashgraph

Nano[37]使用区块点阵(Block Lattice)技术，每个账户都有一条独立的区块链，用户只记录与自己相关的交易，只有自身才能修改记录，完整的交易由发送交易和接收交易两部分组成。交易的收发是异步进行的，发起交易的一方生成一个区块并记录扣除的金额，接收方也生成一个区块并记录收到的金额，实现了瞬时交易。Nano 包含账户持有人(account holder)和代表(representative)两个实体。账户持有人离线时可以选择一名代表进行投票，出现冲突时，由当选的代表创建一个关于交易冲突的投票并收集结果，在投票结束后确认具有最高累积票数(权重)的交易。但是，如果没有足够多的人数来投票解决冲突问题会影响系统的稳定。

2) 收敛的网络拓扑结构

收敛的网络拓扑结构是指区块链中交易按确定的顺序组织或倾向于按确定的顺序收敛。Byteball[38]网络通过可信和有信誉的节点形成特有的主链。这些节点通过周期性地生成见证单元来区分普通节点，如图 12 所示，每个单元都标有主链索引(MCI)，该索引链接到一个见证单元，从而避免冲突。Byteball 网络中通过选举 12 个见证人来避免失败的发生，见证人可以由普通节点代替，新的候选人需要大多数用户达成一致。Conflux[39]提出一种改进的 GHOST(Greedy Heaviest Observed Subtree)算法，引入了自适应权重机制，使得 Conflux 能够在用于快速确认的乐观策略和用于抵抗攻击的保守策略之间切换，以适应不同的工作场景。Conflux 中的每个块都有一个权重，新生成的块将根据其过去的子图自适应地分配权重。

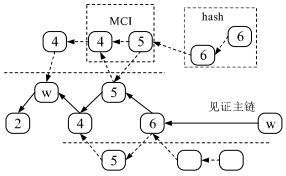

图 12　Byteball 网络

Fig. 12　Byteball

3) 发散的网络拓扑结构

发散的网络拓扑结构是指是指区块链中交易在没有预定顺序的情况下稀疏地分布在不可预测的方向。IOTA[40]采用 UTXO 模型作为数据结构，将节点发布的交易构成了 Tangle 网络。如图 13 所示，IOTA 网络中的所有节点都存储 Tangle 的副本，一个未认证的交易需要指向并认证两个祖先交易，因此，发起交易的用户将有助于系统的安全。Tangle 中的每个节点都代表一个交易，但交易的不断产生容易导致子图向不同方向发散，虽然采用不同的算法来限制子图的发散，但仍可能导致网络分裂成多个孤立的集团。G-IOTA[41]在 IOTA 的基础上进一步完善了激励机制，未确认的交易需要指向并认证三个祖先交易，同时通过引入相互监督的机制，避免节点的作恶。Graphchain[42]的设计与 IOTA 相似，每个交易必须验证多个(至少两个)祖先交易，并引入一种激励机制来维护图形结构，同时交易需要收取交易费用，从而吸引更多的矿工加入区块链网络，以快速确认交易。

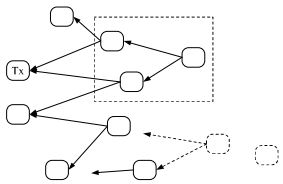

图 13　IOTA 网络

Fig. 13　IOTA

区块链系统的网络拓扑结构是由边和顶点组成的可视化图形，虽然无法确定区块链系统的最终结构，但可以间接反映协议的复杂性。表 3 从区块链的组成单位、共识算法、交易模型、网络拓扑结构、委员会成员选举方式、是否支持智能合约和是否存在激励机制等方面对上述方案进行分析对比。采用平行结构的区块链通过并行处理多条链来横向扩展区块链，使用这种方法的系统一般都有一个固定的安全阈值。在此阈值内，吞吐量可以最大程度地接近通信协议的极限。相反，一旦超过阈值，系统就会受到安全性的限制。因此，在不破坏安全性的情况下提高可扩展性是这一系列研究的关键点。采用收敛结构的区块链主要包括两个步骤，确认主链和交易顺序，主链既能作为可信链记录历史数据，又解决冲突问题。这种方案在比特币的基础架构上进行了改进，采用更复杂的扩展规则来解决分叉问题。这种设计面临与经典区块链系统同样的瓶颈，提高性能依赖于减少主链的确认时间，解决冲突和交易排序的时间成本限制了吞吐量的增长。采用发散结构的区块链是最灵活的区块链系统，没有严格或者统一的共识机制。交易和区块可以任意分散在网络中。每个系统只应用一个简单的规则。这种设计通过减少确认时间提高区块链系统的可扩展性，但是会降低系统系统的安全性或者增加系统的复杂性。此外，由于其非结构化的网络可能会导致过多的随机分叉，从而限制区块链系统性能的提升。

尽管每种类型的系统都截然不同，但它们仍需要在安

全性和可扩展性之间进行权衡。为了实现全局一致性，排序算法可能成为基于 DAG 的区块链系统的瓶颈，排序算法的计算复杂度随着节点数量的增加呈指数增长。小型的委员会使得平行结构的系统更加轻量化，但委员会成员过少或只有一个成员这种特殊的情况，可以最大限度地减少了确认时间，但会引入中心化的风险。弱化对一致性的要求，可以实现高扩展性和快速确认。IOTA 和 Nano 等系统只能保证部分交易的顺序，能够满足两方过多方之间的资产转移，但不支持智能合约。结构良好的 DAG 系统能够快速精确定位特定单元或交易，而发散结构的系统无法精确定位单元或交易。DAG 网络异步处理交易的模式在一定程度上提高了区块链的可扩展性，但仍存在一些缺陷。一方面由于 DAG 的验证规则是后面的交易验证前面的交易，有可能导致最后的交易迟迟无法被验证，甚至在节点数量比较少的情况下，交易时长无法预测，容易带来新的安全问题。另一方面，通过见证人或超级节点原则上可以解决安全问题，但一定程度上违背了去中心化的原则。DAG 技术作为区块链的一个有益补充，其异步通信机制在提高扩展性、缩短确认时间和降低支付费用方面优势明显，但在安全性和一致性方面也有亟待解决的问题。

表 3　DAG 方案对比

Tab. 3　Comparison of DAG schemes

文献	单位	共识机制	交易模型	网络拓扑结构	委员会成员挑选方式	智能合约	激励机制
36	事件	异步 BFT	账户	平行	投票选举	Y	Y
37	交易	DPoS	配对	平行	投票选举	N	N
38	单元	主链 DAG	UTXO	收敛	投票选举	Y	N
39	块	Conflux	UTXO	收敛	PoW	Y	Y
40	包	Tangle	UTXO	发散	-	N	Y
42	交易	Graphchain	UTXO	发散	-	N	Y

2.2　链下扩展

链下扩展和链上扩展是相对的，链下扩展是指在区块链主链之外建立第二层交易网络。链下扩展不直接修改共识机制、区块大小和出块时间等区块链规则，而只将必要的信息记录到区块链上，或在出现数据出错、发生纠纷等情况需要进行验证时才与区块链进行信息交互。因其扩展行为不发生在区块链上，因此被直观地称为链下扩展。链下扩展不受原有区块链性能影响，主要扩展方案包括状态通道、链下计算和链下存储等。

2.2.1　状态通道

状态通道的实现过程可以概括为以下几个步骤：打开状态通道、质押资产、建立一个去中心化的制衡机制、在链下发送交易、对状态签名并发送、双方确认状态的改变、关闭状态通道。状态通道的核心思想是将在链上结算的交易在链下通过状态通道维护中间态，并且在发生纠纷时回到链上仲裁。目前状态通道的主要解决方案有比特币闪电网络(Lightning Network)[43]和以太坊雷电网络(Raiden Network)[44]等。

闪电网络依靠 RSMC(Recoverable Sequence Maturity Contract)和 HTLC(Hashed Time Lock Contract)实现[45]，RSMC 保证了两个人之间的直接交易可以在链下完成，HTLC 保证了任意两人之间的转账都可以通过一条支付通道来完成。具体来说，在支付通道打开后，参与方可离线发送任何数量的交易，无须广播到比特币网络。除最开始创建支付通道和关闭支付通道需要广播上链，中间的交易过程由一系列链下交易记录构成，不需要存储到区块链上。创建支付通道相当于双方各自用一个账本用来记录双方的交易记录，当不想再与对方交易时，可以关闭通道，根据账本中的交易记录进行最终结算和上链。Raiden Network 是状态通道技术在以太坊中的应用，被称为以太坊版本的闪电网络，除了交易细节之外，遵循与闪电网络相同的操作流程和协议。

闪电网络主要应用在微支付场景，如果交易双方之间进行大量的微支付交易，将所有的交易都上链是没有必要的，中间状态可以不用上链，只要所有微支付交易的最终状态上链即可，从而避免高额的交易费用。因为即使所有微支付的交易状态都上链，最后的状态也不发生变化。因此，在链下记录微支付交易的状态信息，只将创建状态及最终状态上链，大量的微支付交易被压缩为少量链上状态，从而提升系统的交易吞吐量。状态通道只在状态通道开启和关闭时向区块链提交信息，具有更快的交易速度和更低廉的交易成本，交易信息只在参与者之间的状态通道中，不会被公开披露，极大提高了隐私和安全性。但状态通道需要实时交互，在大规模应用中可能会出现扩展性问题；另一方面，参与者之间需要相互信任，如果任意一方出现问题，将会导致通道的关闭、资金被锁定或丢失等问题。

2.2.2　链下计算

在区块链系统中，交易信息需要进行全网广播，全网节点基于共识机制处理和验证交易信息，且每个参与节点都保存一份完整的交易历史记录，由此导致区块链系统的性能受到限制。链下计算是通过使用外部资源来减少区块链上的计算工作，将原本置于链上的计算工作，移至链下处理，而链上仅保留验证的部分，以此间接提升链上的数据处理能力。

在以太坊主链执行计算的成本很高，交易由网络上的所有全节点处理，且需要收取高额的 gas 费用，限制了计算能力的提升。Solidity 语言的创始人 Christian Reitwiessner 团队设计了一个降低以太坊网络链上计算负载的智能合约 Truebit[46]。Truebit 将复杂的计算外包给一个可信的第三方，第三方负责执行计算任务并公示运算结果，这一过程称为求解；另一个第三方称为挑战者，验证求解者所做的工作，以此获得奖励。挑战者一定程度上可以避免分歧的出现，降低链上的计算量和 gas 费用，同时能够识别出真实、正确的结果。Arbitrum 方案[47]将智能合约放到链下进行验证，只将处理后的最终结果记录在以太坊链主链，提高区块链的吞吐量。同时设计一种新的虚拟机(Arbitrum Virtual Machine, AVM)用于对不同的智能合约进行隔离和跟踪资源使用情况，出现冲突或争议时，通过二分法定位有争议的指令，识别并奖励诚信的一方、惩罚不诚信的一方。但用户取回资产到以太坊交易的延迟较高，需要一周的挑战期过后才能确认。

Arbitrum 方案和 Truebit 方案都是针对以太坊智能合约

的可扩展性和计算密集型应用程序的解决方案。这两种方案都使用了智能合约和虚拟机来减轻主链上的负载，从而提高可扩展性，但两种方案在实现上有所差异。Truebit 方案引入可信的第三方执行和验证区块链上无法在合适的时间内执行的计算任务，并提供奖励来激励参与者，确保结果的正确性和公正性。Arbitrum 方案采用一种离线验证智能合约的机制，使用虚拟机协议来协调各方的状态。利用各方的数字签名来确认各方是否已经达成一致，以此验证虚拟机状态，通过分叉协议来解决争议，发现并惩罚不诚实的一方。Truebit 方案可以实现更高效的计算，但由于其需要引入第三方求解和验证计算结果，因此可能存在一些安全和信任问题。Arbitrum 方案使用了虚拟机和链下验证的机制，大大降低了验证的负担，提高了智能合约的可扩展性和私密性，但部分参与者作恶可能会影响验证的结果，同时方案设计较为复杂，存在使用难度较高的问题。

尽管链下计算可以提高区块链的可扩展性，但也存在一些局限性。首先，链下计算通常需要依赖中心化的计算节点，这些节点可能受到攻击或崩溃，从而影响整个系统的可靠性和稳定性，这与区块链的去中心化原则不符；其次，计算或验证的结果必须是可信的，以保证整个区块链系统的可靠性，如果链下计算或验证的结果错误或存在欺骗行为，那么整个区块链系统的可靠性也会受到影响；最后，链下计算或验证需要与区块链进行集成，需要额外的开发工作和资源开销，并且会导致系统的复杂性增加。

2.2.3　链下存储

链下存储是指将区块体中数据转移到链下存储系统，区块体中仅存储指向这些数据的“指针”和其他非数据信息[48]，从而降低区块链网络的存储压力。如图 14 所示，存储数据时，将原始数据存放至非区块链系统中，并按照规则生成该数据的唯一标识返回给区块链系统；访问数据时，通过数据的唯一标识在非区块链存储系统中寻找原始数据。以比特币为例，一个区块大小约为 1M，而区块头只有 80byte[49]，将区块体中数据移至链下存储系统链下存储方式，能够极大降低区块链网络的存储压力，根据实现方式和使用的存储系统，目前的链下存储方案可分为基于云的链下存储、基于 DHT 的链下存储和基于 IPFS 的链下存储。

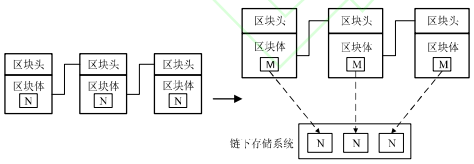

图 14　链下存储

Fig. 14　Off-chain storage

1) 基于云的链下存储

Ali 等学者[50]提出一种去中心化的互联网架构 Blockstack，通过在区块链网络上引入虚拟链(Virtualchain)，把实际数据存放到云端，哈希值保存在区块链，从而提高数据的读写速度。Osei Bryson 等学者[51]选择使用双层区块链结构来处理数据。第一层选用低能耗的主节点和简单的共识机制存储数据，第二层使用 PoW 共识算法用于见证第一层。Xie H 等学者[52]提出一种数据传输结构 HBRSS，将数据划分为块，并将这些块打包形成块环，确保数据的不可窜改和不可破坏，同时使用改进的同态加密算法提高数据的私密性，使得任何第三方都可以快速、安全地处理加密数据，从而在不安全的云环境和通道进行数据传输处理。

2) 基于 DHT 的链下存储

分布式哈希表(Distributed Hash Table, DHT)是一种分布式存储方法[53]。DHT 在网络每个节点存储部分数据并负责一个小范围内的路由，从而实现 DHT 网络的寻址和存储。Zyskind 等学者[54]将 DHT 技术应用到区块链系统中，将数据与数据引用进行分离，数据存储在分布式哈希表中，数据引用存放在区块链上，从而提高区块链系统的可扩展性。文献[55]提出一种新的区块链架构 LightChain，提高区块链网络的通信和存储可扩展性。LightChain 网络不论节点在系统中的影响(如哈希能力、带宽)如何，所有节点都可以参与共识，更去中心化和公平。节点不需要存储完整的交易数据，每个节点只需存储全部块和交易的一个随机子集，并响应其他节点的请求，同时在网络中提供可寻址的节点、块和交易，共同确保数据能够有效的访问。文献[56]提出了一种基于 DHT 的区块链双分片存储扩展机制。结合 DHT 技术和分片技术来实现区块链数据的分片存储，降低节点的存储消耗。通过异或(XOR)运算保证分片被均匀映射到集群中的不同节点进行重叠存储，确保分片数据安全性和可靠性的同时，提高了区块链系统的存储可扩展性。

3) 基于 IPFS 的链下存储

星际文件系统(InterPlanetary File System, IPFS)是一个点对点的分布式文件系统(比特币是一种点对点的电子现金系统)。IPFS 用基于内容的寻址取代传统的基于域名的寻址，如图 15 所示，存放文件时会根据内容计算出的唯一加密哈希值，取回文件时用哈希值根据分布式哈希表找到文件所在的节点，取回并验证文件数据。即用户寻找的不再是某个地址而是储存在某个地方的内容，而且不需要验证发送者的身份，只需要验证内容的哈希。

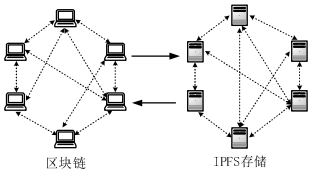

图 15　区块链与 IPFS 交互

Fig. 15　Blockchain interacts with IPFS

文献[57]提出了一种提高物联网流媒体设备可扩展性的方案。通过代理重新加密网络保护物联网流数据，利用 IPFS 来存储和共享物联网流数据，从而解决大型数据的存储问题。用户从链下存储中访问数据，从不可变日志和链上数据的来源检查其完整性，同时为资源受限的物联网流媒体设备开发智能合约，允许物联网设备在链上发送数据块哈希，并将所有数据块存储在链外。最后，通过代理重新加密网络保护物联网流数据的隐私和机密性，所有加密的数据块文件只能进行一次链外写入，但可以多次读取。文献[58]提出了一种基于 IPFS 存储的双区块链系统，用于保护物联网行业的农业采样数据。主链以太坊为公众提供搜索服务，物联网链(ASDC)作为辅链存储农业样本数据。IPFS 网络存储物联网设备收集到的全部数据，同时将数据流重定向到 ASDC 链，ASDC 链将数据存储在块中，并生成块哈希值，这些区块的哈希值被上传到以太坊主链并存储在链上。传统图书馆需要为出版物提供物理存储空间，尽管在计算机的帮助可以进行超高密度的信息存储，但存储和管理成本十分高昂。另一方面，当前主要的信息来源正在从实体图书转向数字图书，面临着记录完整性和存储效率的挑战。文献[59]提出一个基于智能合约和 IPFS 存储方案的电子图书馆系统 LibBlock，以应对数据密度

提高和新兴技术给数字化图书馆带来的挑战。该系统能够高效地存储和分发数据，防止数据冗余和提供安全的访问策略，并为管理者设计特定资源可用的机制，高效整合和利用现有的存储和网络资源，以更低的成本提供更好的服务。

表 4 从链下存储系统的类型、应用场景、链下数据的安全性等方面对链下存储方案进行对比。基于云的链下存储通过云端数据库实现数据的存储和访问，依靠云服务提供商进行数据备份和容灾。基于云的链下存储虽然将存储压力转移到云端，但云存储的通常由中心化的机构提供服务，减弱了区块链去中心化的特性，也无法保证数据的真实性。另一方面，云存储服务的成本也是比较高的，需要衡量降低区块链网络存储压力节省的成本与云存储带来的额外成本的关系，同时云存储带来的开销由谁来负责也是需要思考的问题。与基于云的链下存储方式不同，基于 DHT 的链下存储和基于 IPFS 的链下存储将部分数据迁移到与区块链并行的分布式系统中，基于 DHT 的链下存储通过分布式哈希表实现数据的分布式存储和访问，基于 IPFS 的链下存储通过 IPFS 网络实现数据的内容寻址和分布式存储。这两种方案链下的数据由分布式网络维护，在确保去中心化的同时降低了区块链网络的存储压力，但与传统分布式存储类似，需要冗余存储提高数据的安全性。链下的分布式存储系统可以由区块链网络中的节点和非区块链网络中的节点组成，从而减轻区块链网络中节点的存储压力。但如何确定链下分布式存储系统中区块链节点和非区块链节点的比例是一个关键的问题，因为节点数量和类型的不同会对存储系统的性能和安全性产生重要影响。一方面，区块链节点的数量增长可以提高链下存储系统的安全性和可靠性，但过多的区块链节点可能会导致链下存储系统的性能下降。另一方面，非区块链节点的数量是确保链下存储系统容错性和可扩展性的关键。此外，在确定节点比例时，还需要考虑节点之间的通信和协作问题，以确保链下存储系统的效率和可靠性。链下存储虽然能够极大提高区块链网络的存储可扩展性，但也带来了新的问题。

表 4　链下存储方案对比

Tab. 4　Comparison of off-chain storage solutions

文献	链下存储系统类型	应用场景	链下数据的安全性
50	云存储	去中心化浏览器	云存储服务
51	云存储	访问控制	云存储服务和非对称加密算法
52	云存储	IOT 数据传输	云存储服务和同态加密算法
54	DHT	数据隐私保护	Kademlia 协议
55	DHT	数据存储	DHT 协议
56	DHT	数据存储和保护	Kademlia 协议和分片协议
57	IPFS	IOT 数据存储和共享	IPFS 协议
58	IPFS	数据共享	IPFS 协议
59	IPFS	数据管理	IPFS 协议和智能合约

2.3　基于跨链技术的可扩展

跨链技术是解决两个或多个区块链资产和数据不能转移、传递和交换问题的一种技术。对不同链、链上应用和不同链生态的连通，从根本上解决了不同链之间数据孤岛问题[60]，无形之中成为了提高区块链可扩展性的一种方法。跨链又分为同构链跨链和异构链跨链。同构链即区块链底层技术是相同的，易于跨链的实现；异构链的跨链较为复杂，需要第三方的辅助完成跨链。跨链的过程可分为两个阶段，A 链资产锁定阶段和 B 链相应资产解锁阶段。主要挑战是如何保证 A 链上的资产被锁定，B 链上的资产如何确定解锁，以及如何保证 A 链和 B 链之间资产锁定和解锁的原子性，即对应的资产两条链之间要么锁定和解锁成功，要么锁定和解锁失败。针对以上问题，提出了不同的跨链技术，主要分为 4 类：公证认机制、中继/侧链、哈希锁定和分布式私钥控制。

2.3.1　公证人机制

公证人机制[61]通过引入可信的第三方作为公证人来保证不同链之间资产的转移。如图 16 所示，用户将 A 链的资产转移到公证人的指定的节点进行锁定，确认后，公证人将相应的资产释放到 B 链中用户的地址。公证人机制根据签名方式分为单签名公证人机制、多签名公证人机制和分布式签名公证人机制。多签名公证人机制和分布式签名公证人机制能够避免过渡依赖单个公证人，在少数节点被攻击时不影响系统的稳定性。多签名公证人机制是指通过多个公证人签名确认交易，提高跨链交易的安全性。分布式签名公证人机制实现较为复杂，借鉴多方计算的思想将唯一秘钥拆分为多个碎片，加密后随机分配给多个公证人，只有一定比例的公证人共同签名才能凑出完整秘钥，弱化了公证人在跨链交易中的中心化特性。

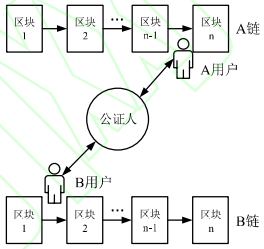

图 16　公证人机制

Fig. 16　Notary mechanism

Interledger[62]是公证人机制的代表性项目之一，设计一个支持不同区块链系统进行资产交易的支付协议。跨链交易引入可信的第三方作为公证人连接两个区块链系统，通过协议对双方交易资产进行托管，公证人达成共识后，交易继续进行，托管的资产才会被释放。Wu 等学者[63]搭建了一个基于周期性委员会轮换机制的异构链通信框架，将公证人机制和中继有机的结合，通过定期重组委员会和优先更换故障节点，保证系统的可靠性。由于引入了委员会作为中继，设计了基于 PBFT 的消息的验证机制，以适应委员会的轮换并提高消息验证的速度。

2.3.2　侧链/中继

侧链[64]最初是为了实现比特币和其他数字货币流通提出的，侧链协议通过互相锚定(如美元锚定黄金)将两条不同的区块链连接起来，使资产能够在不同的区块链之间流通。通常将第一条链称为主链，另一条成为侧链，因两者相互独立，自身链上的创新或更改不会对主/侧链运行造成大的影响。BTC Relay[65]是侧链技术的典型应用，通过以太坊智能合约将以太坊网络连接到比特币网络，允许用户在以太坊上验证比特币交易。中继不同于侧链的双向锚定，而是将中继链作为第三方公证人实现资产交易。如图 17 所示，中继链是在主链和侧链之间之间添加一条区块链来连接两条不同的区块链，通过第三条区块链实现价值和信息的交换。

中继相对于侧链而言更加灵活，应用场景更广泛。微众银行自主研发的跨链交互平台 WeCross[66]，采用基于路由互联的跨链架构，通过跨链接口对智能合约和资产进行抽象的包装，设计出统一的资源范式，解决不同链之间数据结构和不同数据难以互认的问题。最后，基于统一的调用方法，实现不同区块链的统一调用，弱化不同区块链的细节差异。Tendermint 团队设计的异构网络 Cosmos[67]同样基于中继机

制实现跨链交互的。使用基于 PoS 和 BFT 算法改进的 Tendermint 共识算法达成共识，每秒可处理数千笔交易，其严格的问责制度可以在发生分叉时确认责任，防止参与者作恶。如图 18 所示，Cosmos 网络基于 IBC(Inter-Blockchain Communication)协议实现中继通信，为多个不同的区块链互相通信建立信任基础，所有并行链(Zone)的代币可以安全、快速地从一个并行链转移到另一个并行链，同时记录每个并行链代币的数量，从而不依赖受信任的第三方让资产在区块链之间转移。

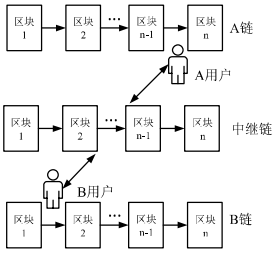

图 17　中继机制

Fig. 17　Relay mechanism

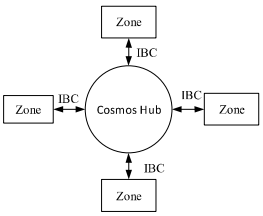

图 18　Cosmos 体系结构

Fig. 18　Cosmos architecture

2.3.3　哈希锁定

哈希锁定(Hashed Time Lock Contract, HTLC)是一种基于原子交换的协议[68]，通过带有哈希锁和时间锁的合约进行资产锁定，设置相应的时间和解锁条件来实现资产交换，超出指定时间后将资产物归原主。哈希锁定无须可信的第三方参与，通过资产质押的方式在不受信任的交易双方之间完成成资产转移，在超时后交易双方能够取回各自的资产，避免拖欠交易，降低交易风险。

哈希锁定机制只支持资产或者信息交换，而不支持资产或者信息的转移。图 19 展示了 A 和 B 交换资产的具体过程。

a) A 随机生成秘钥 s，通过哈希函数得到 s 的哈希值 h，将其发送给 B；

b) A 通过合约锁定 A 链上的资产 x，设置一个锁定时间 T1，解锁条件为 B 获取秘钥 s；

c) B 通过合约锁定在 B 链上得资产，设置一个锁定时间 T2(T2 < T1)，解锁条件为 A 的秘钥 s；

d) A 使用秘钥 s 获取 B 锁定的资产 y；

e) B 使用秘钥 s 获取 A 锁定的资产 x；

交易结束，A 与 B 完成资产转移，如果超时未完成交易，资产会回到各自的账户。

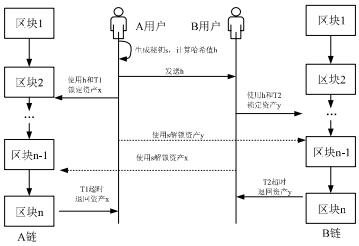

图 19　哈希锁定

Fig. 19　Hash lock

比特币闪电网络是哈希锁定技术的一个典型应用，依靠 RSMC 和 HTLC 实现。RSMC 保证了两个人之间的直接交易可以在链下完成，HTLC 保证了任意两人之间的转账都可以通过一条支付通道来完成[69]。支付通道相当于双方各自用一个账本用来记录交易信息，除创建支付通道和关闭支付通道时需要广播上链，中间的交易过程由一系列链下交易记录构成，不再上链。在支付通道打开后，交易双方可离线发送任意数量的交易，每一笔交易都需要经过交易双方签名认证，交易完成或不再进行交易时关闭通道，最终将经过双方认可的最新交易结果广播上链。

2.3.4　分布式私钥控制

分布式私钥控制[70]是指私有资产通过分布式私钥生成和控制技术映射到一条新的区块链上，在新的链上部署智能合约完成资产交换。分布式私钥控制在分布式签名公证人机制的基础上进一步避免中心化的风险，原始资产从原始链转移到跨链时，跨链节点将向合约指定用户发放相应的等值代币。为确保原始链的资产能够跨链交易引入锁定和解锁技术对资产进行管理，锁定是指使用密钥控制的数字资产进行分布式控制管理和资产映射的过程；解锁是利用分布式私钥对锁定的代币进行解锁操作，将数字资产的控制权返回给所有者。

以 Fusion[71]项目为例，各种加密资产可以通过分布式私钥控制映射到 Fusion 链上，这些资产可以通过合约进行交互。这一过步骤通过 Lock-in(锁定)和 Lock-out(解锁)实现。Lock-in 过程如图 20 所示，用户发起请求，Fusion 把秘钥分片并随机分发给网络中的不同节点，告知用户生成的 Lock-in 地址，用户将指定资产转入生成的 Lock-in 地址中，完成后 Fusion 通过智能合约进行锁定并验证和更新用户的资产信息。Lock-out 阶段用户发起请求后，首先检查映射账户中的信息，满足预设条件后进行秘钥验证，通过后解除控制管理，完成控制权交接后通过智能合约同步更新账户信息记录。

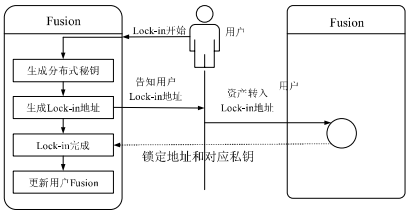

图 20　Fusion 中 Lock-in 过程示意图

Fig. 20　Lock-in process diagram in Fusion

表 5 从安全性、局限性、是否支持智能合约部署、是否需要信任基础、交易速度、互操作性、是否支持跨链资产转移、是否支持跨链资产抵押和典型项目等方面对公证人机制、侧链/中继、哈希锁定分布式私钥控制四种跨链技术进行分析对比。不同的跨链技术在适用的场景、信任基础、支持的功能以及实现难易程度上存在差异。公证人机制和哈希锁定都是较成熟且简单的方案，公证人机制依靠公证人来验证跨链交易的合法性和有效性，引入中心化机构弱化了去中心化的特性。哈希锁定是一种用于验证跨链交易的安全技术，通过将交易哈希值作为锁定条件来确保交易的合法性和有效性，不需要引入第三方机构，相对于公证人机制具有更高的可靠性，但是只支持数字资产的交换。侧链/中继技术通过引入侧链/中继链提高跨链交易的可信度和可靠性，可以将不同区块链之间的数据和资产进行无缝的交换和传递，但侧链/中继技术会增加整个系统的安全风险，在不同的链之间进行交互会引入新的安全问题，同时会涉及用户的隐私问题。分布式私钥控制通过将数字资产的私钥分散存储在多个节点，避免单点故障的同时提高数字资产的安全性，但

需要对私钥的分配、控制和管理进行有效的管理和监控，否则会导致私钥部分丢失或被泄露，秘钥分发需要额外的管理和监控开销，才能确保私钥的安全性和可用性。跨链技术虽然解决了不同链之间数据孤岛问题，但也带来了新的挑战，不同的跨链技术发展的侧重点不同，需要考虑实际的应用场景选用结合不同的技术来解决问题。此外，跨链系统将交易被分散到不同的链上，并行化处理的难度变得更大，同时也对资产的安全和数据的隐私保护提出更高的要求。

表 5　跨链技术对比

Tab. 5　Cross-chain technology comparison

	公证人机制	侧链/中继	哈希锁定	分布式私钥控制
安全性	公证人互相信任	Merkle 证明	哈希算法	多签名算法
局限性	依赖公证人	交易速度慢	应用场景单一	功能单一
智能合约	困难	困难	不支持	支持
信任基础	需要	不需要	不需要	不需要
交易速度	低	低	高	高
互操作性	公证人决定	微支付、合约调用	转账类型交易	转账类型交易
跨链资产转移	支持	支持	不支持	支持
跨链资产抵押	支持	支持	大多数支持	支持
典型项目	Interledger	Cosmos	Lighting network	Fusion

3　总结与展望

本文基于可扩展性角度，从链上、链下、跨链三个方面总结提高区块链可扩展性方法的研究进展，本节分析并指出当前解决方案面临的挑战或存在的一些局限性，并为未来的研究工作提供可能的方向。

3.1　面临的挑战

1) 安全问题

区块链采用一系列密码学算法来确保数据传输安全，但迄今为止其面临的最大挑战仍是安全问题，尤其是公有链，绝大部分链上数据都是公开的。对于链上扩展方式，轻节点与全节点的依赖关系是无可避免的，这时全节点的安全性代表了区块链的安全性，如果全节点作恶，短时间内轻节点容易被欺骗，因此如何提高轻节点的安全性需要更加深入的研究。分片方案通过将区块链网络划分为多个分片，可能存在某些分片中存在大量恶意节点或存在过小的分片，更容易遭受攻击。此外，过多的分片导致交易延迟增长，难以避免双花问题。基于 DAG 的区块链网络拓扑结构较为复杂，存在某些交易长时间无法确认的问题，引入见证人或超级节点带来了中心化的风险。

链下扩展方式将数据移至链下处理，提高了数据泄露的风险。一方面，区块链需要频繁与链下系统交互，信息交互的安全难以保障；另一方面，链下存储方案无法保证链下系统数据的真实性，同时非区块链系统可能非法交易数据谋取利益。跨链扩展方案需要考虑的安全问题更为复杂，公证人信任问题、防止伪造资产转移、交易超时处理、如何保证获取数据的可信和竞争条件攻击等。此外，跨链技术虽然实现了不同链之间的交互，但交易被分散到不同的链上，增加了并行化处理的难度，对资产的安全和数据的隐私保护提出更高的要求。

2) 应用问题

区块链分为公有链、联盟链和私有链。公有链是完全开放的网络，所有用户都可以参与系统维护；联盟链是有限开放的网络，链中的参与方需要事先约定；私有链由个人或者私人机构所有，不对外开放。不同的区块链平台(如超级账本，以太坊)提供不同的服务，不适合所有的应用类型。区块链平台支持的共识算法不同，交易速度不同，都会对应用程序类型产生影响，在不同领域的应用应选用相宜的方案以突出其优势和限制。

链上扩展更适合节点规模较大的公有链和联盟链。轻节点方案更适合便携的小型设备或物联网设备等，虽然许多研究人员提出不依赖全节点的方案，但功能依然无法与全节点相比。分片方案可能导致分片过大或过小，分片过小时只需少量的资源恶意节点就可以完全控制一个分片，为了避免交易涉及到的用户隐私信息泄露给恶意节点，未来的区块链系统需要更多的隐私保护技术，但在采用了隐私保护技术的区块链系统上，如何实现资产以及数据的跨链，将成为一个涉及技术实现和效率的双重问题。是否支持轻客户端对区块链系统的推广至关重要，DAG 网络因其特殊的拓扑机构难以向轻客户端提供证明，目前不支持轻客户端的应用。

状态通道将微支付交易在链下处理，虽然提高了区块链的吞吐量，但只能用于数字支付领域。链下存储方案将数据转移至第三方可信赖的存储系统，减弱了区块链的去中心化特性，不适用于公有链场景；同时查询数据的效率受到链上系统和链下系统交互的影响，不适用于溯源、存证等领域。

跨链技术随着区块链技术的发展而深入，但目前缺乏一个统一的标准。跨链协议为实现不同区块链的互联互通，需要考虑不同区块链的兼容性问题，确保交易能够互相接收。一方面，区块链系统的不断更新，改进共识算法、区块大小和新功能的出现等都会影响跨链协议的兼容性；另一方面，多个区块链相互连接将导致区块链系统整体的复杂度上升。此外，最初许多区块链在设计时并未考虑跨链应用，这些因素都会影响跨链技术的应用。

3) 效率问题

随着区块链数据的不断增长，查找数据的效率会变的越来越低。特别是链下存储方案，需要到非区块链系统检索数据，如果存在恶意节点不仅会返回错误信息，还会影响查询的准确性。因此，在提高区块链可扩展性的同时需要更高效的数据查询方法。

分片是提高区块链可扩展性广泛采用的方法之一，区块链的吞吐量与分片的数量成正比，但分片数量的增加也会降低每个分片的资源和计算能力。当分片过小时，恶意攻击者只需少量的资源就可以完全控制一个分片。因此，需要大量的研究优化分片数量更有效的扩展区块链网络。

各种基于分片的解决方案，如 Elastic、Omniledger 和

Rapidchain 等。虽然实现了低延迟、高吞吐量、存储可扩展和拜占庭容错等目标，但增加了消息的复杂度。在这些方案中，只有 Rapidchain 在不牺牲安全性的情况下能够提供更好的可扩展性，消息复杂度为 O(n)，如何降低区块链内部的消息复杂度，尤其在分片内部，是需要进一步探索的领域。

3.2　未来研究方向

1) 研究更高效的的安全机制

现阶段的解决方案仍存在一些安全问题，轻节点方案需要保证轻节点与全节点信息交互的安全；分片过小易遭受攻击；链下系统与链上系统交互的安全；跨链交互的安全等。另一方面，量子计算机的不断发展也给经典密码学造成冲击和挑战，设计能够抵御量子攻击的密码系统也是需要考虑的问题。因此需要研究更高效或更有针对性的安全机制。

2) 研究分叉监测委员会机制

分叉的形成也是限制区块链可扩展性的原因之一，通常采用最长链原则处理这些分叉。但如果没有合适机制的避免分叉出现，仍会浪费大量的资源，从而影响区块链的整体性能。针对这一问题可以建立分叉监测委员会(可以由激励节点组成)，委员会与矿工节点是分离的，由委员会持续监测分叉的形成。

3) 研究信誉管理方法和负载平衡机制

交易通信成本指的是完成一次交易所需的通信费用，现有的解决方案，为了降低交易通信成本，要么牺牲可靠性和区块链的去中心化性质，依赖可信任的硬件，要么假设所有节点都被激励且无作恶行为。可以探索部署分散信誉管理方法和负载平衡机制，并采用更具吸引力的激励策略，防止不受信任的节点或没有可信硬件的节点的异常行为。

4) 研究更具普适性的通用跨链体系架构

随着区块链技术在不同场景的应用，跨链技术也得到进一步的发展。区块链互操作性需要建立标准化的体系架构，不兼容的标准会阻碍区块链互操作性的发展，没有标准的跨链工作联通困难、难以监管。跨链技术在降低跨链机制中心化、减轻主链负担方面可以进行更深入的探索和研究。

4　结束语

区块链是一种新型的分布式计算基础平台，具有以前计算平台所不具备的技术优势，其相关的理论和技术备受研究人员的关注。随着区块链技术的快速发展，区块链的可扩展性已成为制约区块链大规模应用的阻碍，为了推动传统行业进行数字化转型，构建信任体系，促进行业发展，研究区块链的可扩展性问题是很有必要的。本文从扩展性角度出发，首先介绍分布式系统的可扩展性，其次分析了链上、链下和跨链三类提高区块链可扩展性技术的研究进展，最后阐述对提高区块链可扩展性技术所面临挑战的思考和总结。

参考文献：

[1] Vacca A, Di Sorbo A, Visaggio C A, *et al.* A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges [J]. Journal of Systems and Software, 2021, 174: 110891.

[2] 邵奇峰, 张召, 朱燕超, 等. 企业级区块链技术综述 [J]. 软件学报, 2019, 30 (09): 2571-2592. (Shao Qifeng, Zhang Zhao, Zhu Yanchao, *et al.* Survey of enterprise blockchains [J]. Journal of Software, 2019, 30 (9): 2571−2592)

[3] Berdik D, Otoum S, Schmidt N, *et al.* A survey on blockchain for information systems management and security [J]. Information Processing & Management, 2021, 58 (1): 102397.

[4] 刘双印, 雷墨鹭兮, 王璐, 等. 区块链关键技术及存在问题研究综述 [J]. 计算机工程与应用, 2022, 58 (03): 66-82. (Liu Shuangyin, Lei Moyixi, Wang Lu, *et al.* Survey of blockchain key technologies and existing problems [J]. Computer Engineering and Applications, 2022, 58 (03): 66-82.)

[5] 邓小鸿, 王智强, 李娟, 等. 主流区块链共识算法对比研究 [J]. 计算机应用研究, 2022, 39 (01): 1-8. (Deng Xiaohong, Wang Zhiqiang, Li Juan, *et al.* Comparative research on mainstream blockchain consensus algorithms [J]. Application Research of Computers, 2022, 39 (01): 1-8.)

[6] Singh S, Hosen A S M S, Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed iot network [J]. IEEE Access, 2021, 9: 13938-13959.

[7] 朱盼盼, 张彤, 郑宇宁, 等. 分布式存储系统中纠删码数据修复算法优化与实现 [J]. 计算机应用研究, 2020, 37 (S1): 140-142. (Zhu Panpan, Zhang Tong, Zheng Yuning, *et al.* Optimization and implementation of erasure code data repair algorithm in distributed storage system [J]. Application Research of Computers, 2020, 37 (S1): 140-142.)

[8] Sadeeq M A, Zeebaree S. Energy management for internet of things via distributed systems [J]. Journal of Applied Science and Technology Trends, 2021, 2 (2): 59-71.

[9] Hakim D K, Riyanto J K, Fauzan A. Pengujian Algoritma Load Balancing pada Virtualisasi Server [J]. Sainteks, 2020, 16 (1) .

[10] 高晶, 王粟. 数据库技术的发展现状与趋势研究 [J]. 无线互联科技, 2018, 15 (03): 35-37. (Gao Jin, Wang Su. Study on the development status and trend of database technology [J]. Wireless Internet Technology, 2018, 15 (03): 35-37.)

[11] 田真真, 蒋维, 郑炳旭, 等. 基于服务器集群的负载均衡优化调度算法 [J]. 计算机科学, 2022, 49 (S1): 639-644. (Tian Zhenzhen, Jiang Wei, Zheng BingXu, *et al.* Load balancing optimization scheduling algorithm based on server cluste [J]. Computer Science, 2022, 49 (S1): 639-644.)

[12] Atto K, Kotova E E. Communicative Strategies Simulation in Intelligent Learning Environment [C]// Proc of IEEE the 3th Communication Strategies in Digital Society Seminar (ComSDS) . IEEE, 2020: 37-39.

[13] 朱涛, 郭进伟, 周欢, 等, 周傲英. 分布式数据库中一致性与可用性的关系 [J]. 软件学报, 2018, 29 (01): 131-149. (Zhu Tao, Guo Jinwei, Zhou Huan, *et al.* Consistency and availability in distributed database systems [J]. Journal of Software, 2018, 29 (01): 131-149.)

[14] 潘恒, 钱海洋, 姚中原, 等. 典型区块链存储与查询技术综述 [J]. 郑州大学学报: 理学版, 2022, 54 (06): 34-50. (Pan Heng, Qian Haiyang, Yao Zhongyuan, *et al.* A Survey of typical blockchain storage and query technologies [J]. Journal of Zhengzhou University: Natural Science Edition, 2022, 54 (06): 34-50.)

[15] 傅丽玉, 陆歌皓, 吴义明, 等. 区块链技术的研究及其发展综述 [J]. 计算机科学, 2022, 49 (S1): 447-461+666. (Fu Liyu, Lu Gehao, Wu Yiming, *et al.* Overview of eesearch and development of blockchain technology [J]. Computer Science, 2022, 49 (S1): 447-461+666.)

[16] Thakkar P, Nathan S, Viswanathan B. Performance benchmarking and optimizing hyperledger fabric blockchain platform [C]// Proc of IEEE the 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS) . IEEE, 2018: 264-276.

[17] Sanka A I, Cheung R C C. A systematic review of blockchain scalability: Issues, solutions, analysis and future research [J]. Journal of Network and

Computer Applications, 2021, 195: 103232.

[18] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [J]. Decentralized Business Review, 2008: 21260.

[19] Kiayias A, Miller A, Zindros D. Non-interactive proofs of proof-of-work [C]// Proc of the 24th International Conference on Financial Cryptography and Data Security. Springer, Cham, 2020: 505-522.

[20] Bünz B, Kiffer L, Luu L, *et al.* Flyclient: Super-light clients for cryptocurrencies [C]// Proc of the 41th IEEE Symposium on Security and Privacy (SP) . IEEE, 2020: 928-946.

[21] Maalla M A, Bezzateev S V. Efficient incremental hash chain with probabilistic filter-based method to update blockchain light nodes [J]. Научно-технический вестник информационных технологий, механики и оптики, 2022, 22 (3): 538-546.

[22] Kim T, Noh J, Cho S. SCC: Storage compression consensus for blockchain in lightweight IoT network [C]// Proc of IEEE the 37th International Conference on Consumer Electronics (ICCE) . IEEE, 2019: 1-4.

[23] Nagayama R, Banno R, Shudo K. Trail: A Blockchain Architecture for Light Nodes [C]// Proc of IEEE the 25th Symposium on Computers and Communications (ISCC) . IEEE, 2020: 1-7.

[24] 李国，殷俊锋，李静. LS&SSS-RS：可更新密钥分片的数据安全散布方法 [J]. 计算机应用研究, 2021, 38 (05): 1533-1538. (Li Guo, Yin Junfeng, Li Jing. LS&SSS-RS: updatable key sharding method for data secu-rity dissemination [J]. Application Research of Computers, 2021, 38 (05): 1533-1538.)

[25] 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 (06): 1-10. (Huang Huawei, Kong wei, Peng Xiaowen, *et al.* Survey on blockchain sharding technology [J]. Computer Engineering, 2022, 48 (06): 1-10.)

[26] Luu L, Narayanan V, Zheng C, *et al.* A secure sharding protocol for open blockchains [C]// Proc of the 23th ACM SIGSAC conference on computer and communications security. 2016: 17-30.

[27] Kogias E K, Jovanovic P, Gailly N, *et al.* Enhancing bitcoin security and performance with strong consistency via collective signing [C]// Proc of the 25th usenix security symposium (usenix security 16) . 2016: 279-296.

[28] Gilad Y, Hemo R, Micali S, *et al.* Algorand: Scaling byzantine agreements for cryptocurrencies [C]// Proc of the 26th symposium on operating systems principles. 2017: 51-68.

[29] 汪浩，姜顺，潘丰. 基于 Round-Robin 协议网络化系统的故障检测 [J]. 信息与控制, 2019, 48 (05): 595-602. (Wang Hao, Jiang Shun, Pan Feng. Fault detection for networked control systems based on Round-Robin protocol [J]. Information and Control, 2019, 48 (05): 595-602.)

[30] Zamani M, Movahedi M, Raykova M. Rapidchain: Scaling blockchain via full sharding [C]// Proc of the 25th ACM SIGSAC conference on computer and communications security. 2018: 931-948.

[31] Kanso A, Ghebleh M. A trapdoor one-way function for verifiable secret sharing [J]. High-Confidence Computing, 2022, 2 (2): 100060.

[32] Han R, Yu J, Lin H, *et al.* On the security and performance of blockchain sharding [J]. Cryptology ePrint Archive, 2021.

[33] Hafid A, Hafid A S, Samih M. New mathematical model to analyze security of sharding-based blockchain protocols [J]. IEEE Access, 2019, 7: 185447-185457.

[34] Tao Y, Li B, Jiang J, *et al.* On sharding open blockchains with smart contracts [C]// Proc of IEEE the 36th International Conference on Data Engineering (ICDE) . IEEE, 2020: 1357-1368.

[35] Wang J, Wang H. Monoxide: Scale out Blockchains with Asynchronous Consensus Zones [C]// Proc of the 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI) , 2019: 95-112.

[36] Baird L, Harmon M, Madsen P. Hedera: A governing council & public hashgraph network [J]. The trust layer of the internet, whitepaper, 2018, 1: 1-97.

[37] LeMahieu C. Nano: A feeless distributed cryptocurrency network [J]. Nano whitepaper, 2018, 4.

[38] Dong Z, Zheng E, Choon Y, *et al.* Dagbench: A performance evaluation framework for dag distributed ledgers [C]// Proc of IEEE the 12th international conference on cloud computing (CLOUD) . IEEE, 2019: 264-271.

[39] Li C, Li P, Zhou D, *et al.* A decentralized blockchain with high throughput and fast confirmation [C]// Proc of the 31th{USENIX}Annual Technical Conference ({USENIX}{ATC}20) . 2020: 515-528.

[40] 田志宏，赵金东. 面向物联网的区块链共识机制综述 [J]. 计算机应用, 2021, 41 (04): 917-929. (Tian Zhihong, Zhao Jindong. Overview of blockchain consensus mechanism for internet of things [J]. Journal of Computer Applications, 2021, 41 (04): 917-929.)

[41] Bu G, Gürcan Ö, Potop-Butucaru M. G-IOTA: Fair and confidence aware tangle [C]// Proc of IEEE the 12th Conference on Computer Communications Workshops (INFOCOM WKSHPS) . IEEE, 2019: 644-649.

[42] Tomaszuk D, Kuziński D, Sopek M, *et al.* A distributed graph data storage in ethereum ecosystem [C]// Proc of the 18th Economics of Grids, Clouds, Systems, and Services, GECON 2021, Virtual Event, September 21–23, 2021, Proceedings. Cham: Springer International Publishing, 2021: 223-231.

[43] 陈艳姣，朱笑天，于永瑞，等. 区块链闪电网络实证分析：拓扑、发展和收费策略 [J]. 软件学报, 2022, 33 (10): 3858-3873. (Chen Yanjiao, Zhu Xiaotian, Yu Yongrui, *et al.* Empirical analysis of lightning network: topology, evolution, and fees [J]. Journal of Software, 2022, 33 (10): 3858-3873.)

[44] Kim S, Kwon Y, Cho S. A survey of scalability solutions on blockchain [C]// Proc of the 9th International Conference on Information and Communication Technology Convergence (ICTC) . IEEE, 2018: 1204-1207.

[45] Que P, Zeng Y, Gao F. The Current Situation and Prospect of the Development of Metaverse Technology [C]// Proc of the 4th International Conference on Applied Machine Learning (ICAML) . IEEE, 2022: 1-5.

[46] Teutsch J, Reitwießner C. A scalable verification solution for blockchains [J]. arXiv preprint arXiv: 1908. 04756, 2019.

[47] Kalodner H, Goldfeder S, Chen X, *et al.* Arbitrum: Scalable, private smart contracts [C]// Proc of the 27th USENIX Security Symposium (USENIX Security 18) . 2018: 1353-1370.

[48] 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 (01): 1-20. (Sun Zhixin, Zhang Xin, Xiang Feng, *et al.* Survey of storage scalability on blockchain [J]. Journal of Software, 2021, 32 (1): 1 (20.)

[49] Cao M, Wang H, Yuan T, *et al.* Meta-Regulation: Adaptive Adjustment to Block Size and Creation Interval for Blockchain Systems [J]. IEEE Journal on Selected Areas in Communications, 2022, 40 (12): 3702-3718.

[50] Ali M, Nelson J, Shea R, *et al.* Blockstack: A global naming and storage system secured by blockchains [C]// Proc of the 19th USENIX annual

technical conference (USENIX ATC 16) . 2016: 181-194.

[51] Osei-Bryson K M A. A Blockchain-based Security-Oriented Framework for Cloud Federation [J]. 2018.

[52] Xie H, Zhang Z, Zhang Q, *et al.* HBRSS: Providing high-secure data communication and manipulation in insecure cloud environments [J]. Computer Communications, 2021, 174: 1-12.

[53] Lobo P A, Sarasvathi V. Distributed file storage model using IPFS and blockchain [C]// Proc of the 2th Global Conference for Advancement in Technology (GCAT) . IEEE, 2021: 1-6.

[54] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data [C]// Proc of IEEE the 4th Security and Privacy Workshops. IEEE, 2015: 180-184.

[55] Hassanzadeh-Nazarabadi Y, Küpçü A, Özkasap Ö. Lightchain: Scalable dht-based blockchain [J]. IEEE Trans on Parallel and Distributed Systems, 2021, 32 (10): 2582-2593.

[56] Zhao J, Zhang D, Liu W, *et al.* DHT-Based Blockchain Dual-Sharding Storage Extension Mechanism [J]. Applied Sciences, 2022, 12 (19): 9635.

[57] Hasan H R, Salah K, Yaqoob I, *et al.* Trustworthy iot data streaming using blockchain and ipfs [J]. IEEE Access, 2022, 10: 17707-17721.

[58] Ren W, Wan X, Gan P. A double-blockchain solution for agricultural sampled data security in Internet of Things network [J]. Future Generation Computer Systems, 2021, 117: 453-461.

[59] Chiu W Y, Meng W, Li W. LibBlock-Towards Decentralized Library System based on Blockchain and IPFS [C]// Proc of the 18th International Conference on Privacy, Security and Trust (PST) . IEEE, 2021: 1-9.

[60] 孟博, 王乙丙, 赵璨, 等. 区块链跨链协议综述 [J]. 计算机科学与探索, 2022, 16 (10): 2177-2192. (Meng Bo, Wang Yibing, Zhao Can, *et al.* Survey on cross-chain protocols of blockchain [J]. Journal of Frontiers of Computer Science and Technology, 2022, 16 (10): 2177-2192.)

[61] Pillai B, Biswas K, Muthukkumarasamy V. Cross-chain interoperability among blockchain-based systems using transactions [J]. The Knowledge Engineering Review, 2020, 35.

[62] 孙浩, 毛瀚宇, 张岩峰, 等. 区块链跨链技术发展及应用 [J]. 计算机科学, 2022, 49 (05): 287-295. (Sun Hao, Mao Hanyu, Zhang Yanfeng, *et al.* Development and application of blockchain cross-chain technology [J]. ComputerScience, 2022, 49 (05): 287-295.)

[63] Wu Z, Xiao Y, Zhou E, *et al.* A Solution to Data Accessibility Across Heterogeneous Blockchains [C]// Proc of IEEE the 26th International Conference on Parallel and Distributed Systems (ICPADS) . IEEE, 2020: 414-421.

[64] Cao L, Song B. Blockchain cross-chain protocol and platform research and development [C]// International Conference on Electronics, Circuits and Information Engineering (ECIE) . IEEE, 2021: 264-269.

[65] Guo Z, Liu L, Liang Z, *et al.* Blockchain cross-chain technology research [C]// Proc of IEEE the 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) . IEEE, 2022, 5: 1064-1070.

[66] WANG C, JIANG H, ZENG J, *et al.* A Review of Blockchain Layered Architecture and Technology Application Research [J]. Wuhan University Journal of Natural Sciences, 2021, 26 (5): 416.

[67] Han J, Kim J, Youn A, *et al.* Cos-CBDC: Design and Implementation of CBDC on Cosmos Blockchain [C]// Proc of the 22th Asia-Pacific Network Operations and Management Symposium (APNOMS) . IEEE, 2021: 303-308.

[68] Lan R, Upadhyaya G, Tse S, *et al.* Horizon: A gas-efficient, trustless bridge for cross-chain transactions [J]. arXiv preprint arXiv: 2101. 06000, 2021.

[69] Wu J, Jiang S. On Increasing Scalability and Liquidation of Lightning Networks for Blockchains [J]. IEEE Trans on Network Science and Engineering, 2022, 9 (4): 2589-2600.

[70] 叶祥翮, 刘学业, 王斌辉, 等. 面向联盟链的分布式公证人跨链模型 [J]. 应用科学学报, 2022, 40 (04): 567-582. (Ye Xianghe, Liu Xueye, Wang Binhui, *et al.* Distributed notary cross-chain model for consortium chain [J]. Journal of Applied Sciences, 2022, 40 (04): 567-582.)

[71] Cao L, Song B. Blockchain cross-chain protocol and platform research and development [C]// International Conference on Electronics, Circuits and Information Engineering (ECIE) . IEEE, 2021: 264-269.