软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2024,35(2):828−851 [doi: 10.13328/j.cnki.jos.006954]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链扩展技术现状与展望*

陈 晶, 杨 浩, 何 琨, 李 凯, 加 梦, 杜瑞颖

(空天信息安全与可信计算教育部重点实验室 (武汉大学 国家网络安全学院), 湖北 武汉 430072)

通信作者: 陈晶, E-mail: chenjing@whu.edu.cn

摘　要: 近年来, 区块链技术引起广泛关注, 其作为一种分布式账本技术, 由于具备开放性、透明性和不可篡改性, 已经被应用到诸多领域. 但随着用户数量和访问需求的大幅增加, 现有区块链体系结构可扩展性不足导致的性能瓶颈, 制约了区块链技术的应用和推广, 如何解决可扩展性问题已成为学术界和工业界关注的热点. 对已有的区块链扩展方案进行分析和总结. 首先, 介绍区块链基本概念和可扩展性问题的由来, 定义可扩展性问题并提出衡量可扩展性的指标. 其次, 给出分类框架, 将现有方案按网络扩展、链上扩展、链下扩展 3 大类进行介绍, 通过对不同的区块链可扩展性方案进行分析, 比较各自的技术特点并归纳优缺点. 最后, 对亟待解决的开放性问题进行讨论, 展望区块链技术未来趋势.

关键词: 区块链; 可扩展性; 交易吞吐量; 区块链体系结构; 区块链共识

中图法分类号: TP393

中文引用格式: 陈晶, 杨浩, 何琨, 李凯, 加梦, 杜瑞颖. 区块链扩展技术现状与展望. 软件学报, 2024, 35(2): 828–851. http://www.jos.org.cn/1000-9825/6954.htm

英文引用格式: Chen J, Yang H, He K, Li K, Jia M, Du RY. Current Situation and Prospect of Blockchain Scaling Technology. Ruan Jian Xue Bao/Journal of Software, 2024, 35(2): 828−851 (in Chinese). http://www.jos.org.cn/1000-9825/6954.htm

Current Situation and Prospect of Blockchain Scaling Technology

CHEN Jing, YANG Hao, HE Kun, LI Kai, JIA Meng, DU Rui-Ying

(Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education (School of Cyber Science and Engineering, Wuhan University), Wuhan 430072, China)

Abstract: In recent years, blockchain technology has attracted a lot of attention. As a distributed ledger technology, it has been applied to many fields due to its openness, transparency, and non-tamperability. However, as the number of users and access requirements rise, the performance bottleneck induced by the poor scalability of the existing blockchain architectures has restricted the application and promotion of blockchain technology. How to solve the scalability problem has become a hotspot issue in academia and industry. This study analyzes and summarizes the currently available blockchain scaling solutions. For this purpose, the study outlines the basic concept of blockchain and the origin of the scalability problem, defines the scalability problem, and proposes the metrics for scalability. Then, it presents a classification framework and reports the existing solutions in the manner of categorizing them into three classes: network scaling, on-chain scaling, and off-chain scaling. Different blockchain scalability solutions are analyzed for a comparison of their respective technical characteristics and a summary of their advantages and disadvantages. Finally, this study discusses the open issues that need to be addressed promptly and explores the future trends of blockchain technology.

Key words: blockchain; scalability; transaction throughput; blockchain architecture; blockchain consensus

区块链技术起源于 2008 年中本聪提出的比特币[1], 是一种不需要依赖任何可信第三方的分布式账本. 区块链技术自诞生以来发展十分迅速, 由于具有公开透明、非中心化、不可篡改等特性, 区块链已经被广泛应用到各行

* 基金项目: 国家重点研发计划 (2021YFB2700200); 中央高校基本科研业务费 (2042022kf1195, 2042022kf0046); 国家自然科学基金 (62076187, 62172303); 湖北省重点研发计划 (2022BAA039); 山东省重点研发计划 (2022CXPT055)
收稿时间: 2022-12-11; 修改时间: 2023-01-20, 2023-03-01; 采用时间: 2023-03-30; jos 在线出版时间: 2023-11-08
CNKI 网络首发时间: 2023-11-10

各业, 包括医疗健康[2]、金融行业[1,3]、政府部门[4]、人工智能[5]以及物联网[6,7]等. 即使区块链拥有很多优秀的特性, 但是当用户数量和访问需求大幅增加时, 当前的区块链系统难以达到和传统中心化系统一样的效率. 目前主流的公有链如比特币[1]产生一个区块的平均间隔为 10 min, 理论上每秒最多只能处理 7 笔交易, 以太坊支持大约每秒 25 笔交易[8]. 主流的联盟链 HyperLedger Fabric[9]每秒最多可处理约 1 500 笔交易. 已有区块链系统的性能和 Visa 卡几万的吞吐量以及支付宝几十万的吞吐量相差甚远. 区块链系统的性能难以满足许多业务场景的实际应用需求, 尤其是需要高频交易的场景. 例如现实生活中双十一网络购物这种高频交易场景, 大型云服务器数据在区块链上安全存储, 区块链需要有能力存储庞大数据流等场景都要求对区块链进行扩展. 其本质上是区块链可扩展性不足而导致的性能瓶颈问题. 如何增强区块链的可扩展性是提高区块链性能的关键, 也是当前区块链领域最为重要的研究方向之一.

虽然, 当前部分文献对区块链的性能提升方案进行了综述, 但是按照区块链的 6 层结构来看, 已有工作对可扩展性的分析都不够全面. 文献 [10] 进行了大量的调研, 但多集中于合约层和应用层, 主要关注侧链技术. 文献 [11] 比较了大量链上和链下扩容方案, 文献 [12] 则关注共识层的相关协议的比较以及网络传输效率相关的方案. 文献 [13] 的分析涉及数据层和共识层等, 对比特币、以太坊和有向无环图结构的方案进行性能比较, 但是其调研的文献数量较少, 文献 [14] 梳理当下主流区块链扩容技术, 对扩容技术方案进行了详细清晰的分类, 该工作侧重于整体层面研究, 对每一类共识机制的介绍过于简单. 区块链可扩展性涉及体系结构设计, 仅对部分层的分析显然是不够的. 由于仅关注于某一类问题, 已有的综述对可扩展性的定义不完备, 无法给出通用的分类方法. 并且, 已有工作没有统一的衡量标准来对多个层次的可扩展性方案进行比较.

本文从区块链的体系结构出发, 全面调研了可以提升区块链可扩展性的多种方案, 旨在通过分析各种技术方向的优缺点以进一步剖析区块链的可扩展性问题. 本文基于体系结构, 从网络层、链上层、链下层这 3 个层面更广泛地定义区块链可扩展性问题, 并将已有方案分为网络层方案、链上层方案、链下层方案这 3 种类型. 在这 3 种类型内又进一步细化归纳, 分析比较各个方案的特点. 此外, 本文展开了开放性问题, 宏观讨论现有工作的不足以及未来的研究方向. 本文的主要贡献如下.

- 从网络层、链上层、链下层这 3 个方面更充分地定义可扩展性, 提出可以衡量可扩展性的通用指标.
- 提出对可扩展性方案通用的分类框架, 将现有方案分为提升底层区块链网络性能网络扩展, 优化区块链自身属性的链上扩展, 扩充区块链功能的链下扩展这 3 大类型.
- 总结各类可扩展性解决方案的特点, 并进行分析对比. 并对区块链可扩展性的未来研究方向进行开放性讨论.

本文第 1 节解释区块链的一些基本概念和术语. 第 2 节定义可扩展性问题并提取通用的衡量指标. 第 3 节给出可扩展性通用分类框架, 并对每一类技术方案进行分析对比. 第 4 节汇总比较可扩展性技术, 并进行更宏观的开放性问题讨论.

1 区块链基本概念

本节介绍一些区块链基本的术语和概念.

区块链 (C): 一种公共账本, 是一个不断增长的数据集合, 其中包含所有已经完成的区块. 由于不断地有区块产生, 并且按照时间顺序线性地添加到这个公共账本中, 所以其数据量在不断增加.

交易 (Tx): 一个数据结构, 指的是在没有第三方干预的情况下, 参与区块链系统的两个或者多个用户之间的数据交换. 每笔交易都记录在区块链中, 换句话说, 一笔交易可以被看作是称作区块链的全局账本中的一个条目.

区块 (B): 一个数据结构, 包含区块头和区块体. 区块头记录区块链的状态信息, 链接上一个区块, 提供完整性校验, 区块体主要包含交易数据.

区块链成员 (P): 区块链成员可以分为用户和矿工, 用户负责产生交易, 矿工负责区块链的创建与维护, 并且通过共同协商创建区块, 并将其添加到区块链中.

交易池 ($TxPool$): 交易池是包含所有交易的缓存池, 区块链成员用这些交易进行区块的生成.

共识机制 ($Fcons$): 区块链系统由于不存在中心化机制, 进行状态更新时需要一种区块链成员之间的协商与

认可机制, 如工作量证明 (poof of work, PoW) 通过证明完成计算来竞争区块链的更新权力, 即记录交易的权力.

基础的区块链架构至少需要包含存放区块链各种信息的数据层、完成区块链系统数据交换的网络层、保证区块链系统信息交互一致共识层. 数据层主要包含区块 B 和交易 Tx 两种数据结构. $C=\{B_0,B_1,B_2,B_3,B_4,\ldots,B_n\}$ 表示一条区块链, 区块 B 是区块链的基本组成单位, 多个区块进行有序组织构成区块链. 区块 B 包含验证信息 $VefMsg$ 和数据信息 $Set<Tx_0,Tx_1,\ldots,Tx_k>$, 验证信息用于更新区块链状态和维持完整性, 数据信息主要指交易构成的集合, 所以 $B=\{VefMsg,Set<Tx_0,Tx_1,\ldots,Tx_k>\}$, 其中 k 为区块能包含的最大交易数. 在网络层, 区块链需要建立分布式的对等网络, 采用无许可的网络环境时, 任何分布式网络节点都可以充当区块链成员 P 中的矿工. 矿工从交易池收集交易打包产生区块, 交易池指的是未被打包的交易构成的集合, $TxPool=Set<preTx_0,preTx_1,\ldots,preTx_m>$, 其中 m 为交易池中交易的最大数目, $preTx$ 表示未被打包的交易, 当矿工收集交易并确认上链后, 会从交易池移除该交易. 在共识层, 对于新产生的区块, 其是否能够加入系统需要区块链成员之间达成一致, 在分布式环境下需要一个共识机制 $Fcons$ 来保证决策的可靠性, 这个机制可以抽象为一个实现分布式成员之间信息交互一致性的方法. 在基础的区块链架构之上, 还需要维持参与者稳定工作的激励层, 积极有效的激励机制往往有助于保证区块链系统平稳运行和抵抗恶意行为. 并且, 在基础的区块链之上建立智能合约使得交易账本可实现更复杂的交互行为. 由此, 区块链系统可以从单纯的交易账本变为运行程序代码的合约平台, 可以进一步地实现链上链下融合和多链交互, 提升区块链的应用性.

2 可扩展性定义和衡量指标

分布式系统的可扩展性指的是系统为了满足新增的需求时对系统本身的改动程度. 区块链的可扩展性指的无论交易量和成员数量, 区块链系统对于交易的处理能力. 如果一个区块链的性能能够随着用户需求而增长, 认为其是可扩展的. 为了进一步理解可扩展性问题, 本文从以下 3 个方面更具体地定义区块链可扩展性.

(1) 网络层: 区块链建立在通信网络之上, 优化区块链的底层信息传递网络可以提升区块链信息的传输效率, 改善区块链的可扩展性, 所以对区块链底层网络协议的优化可以提高区块链可扩展性.

(2) 链上层: 区块链自身的设计属性很大程度决定其性能, 主要体现在区块大小、节点组织、共识机制及区块链结构等方面, 所以对区块链自身设计属性的扩展可以提高区块链可扩展性.

(3) 链下层: 不同的场景有不同的用户数量和访问需求, 除了效率之外, 为了更广泛地应用于多个场景, 区块链系统需要在频繁交易、复杂计算和多链联合等方面进行功能性扩展, 所以对区块链功能的拓展可以提高区块链可扩展性.

区块链应该具备处理网络中大量的用户需求和交易的能力, 但这无法由系统的单个性质决定, 由多个指标共同体现. 本文基于上述可扩展性定义提出用于衡量区块链系统的可扩展性的指标.

吞吐量: 单位时间内区块链系统可以处理 (在全网达成共识) 的事务数量 (transactions per second, TPS).

延迟: 区块链系统内一个事务从被用户提出, 到最终在全网达成共识所花费的时间.

成本: 整个区块链系统为了达成共识, 所有节点耗费的通信资源 (通信复杂度), 计算资源 (计算时间), 存储资源 (存储空间).

安全性: 包括整个区块链系统能够容忍恶意节点占总节点数量的比例, 区块链系统能够容忍敌手的控制节点的能力 (静态敌手一旦协议开始后选定哪些节点为恶意节点, 之后就无法随意控制其他节点变为恶意节点, 自适应敌手在协议运行过程中可以随意控制哪些节点变为恶意节点), 对一些攻击的防御 (例如双花攻击和审查攻击).

非中心化: 指区块链的设计结构上对中心化节点或者中心化机构的依赖程度, 例如比特币没有中心化节点, 所以去中心化程度很高. 分片结构的区块链片之间通讯需要依赖跨片节点, 所以依赖中心化节点, 去中心化程度一般. 而联盟链很大程度依赖中心化节点群或者中心化机构, 去中心化程度很低.

3 分类框架及已有方案分析

区块链是基于网络搭建的, 根据开放式系统互联模型 (open system interconnection reference model, OSI) 将网

络划分为 7 层结构, 分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层. 在此基础上区块链模型是一个 6 层结构, 自底向上依次是数据层、网络层、共识层、激励层、合约层和应用层. 依据第 3 节的可扩展性这 3 个方面将现有的可扩展性解决方案归类为优化底层网络传输的网络扩展、针对区块链内部属性的链上扩展、针对区块链外部功能的链下扩展这 3 类, 实际上它们对应区块链层级也是自底向上的. 可扩展性方案分类和网络分层及区块链分层架构的对应关系如图 1 所示. 对于区块链面临的存储可扩展问题和模型归纳如表 1 所示.

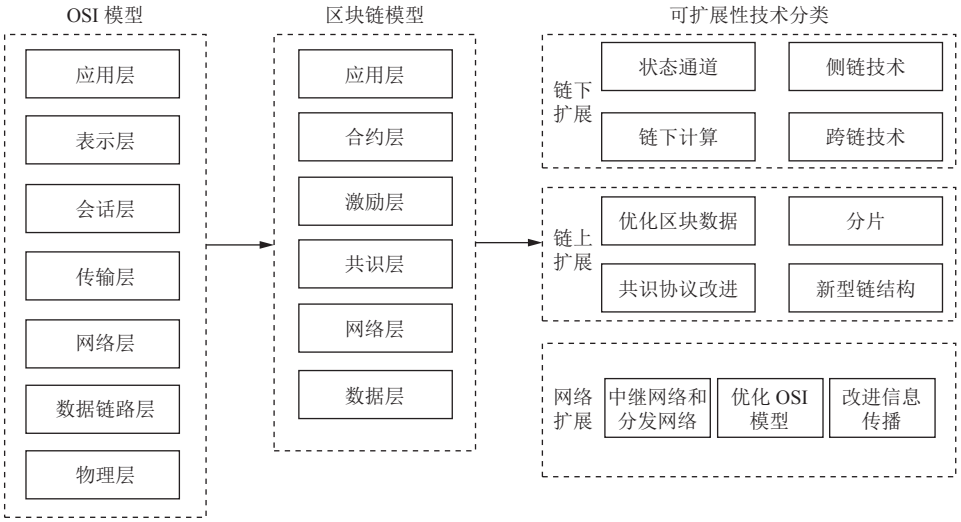

图 1　体系架构与可扩展性技术分类

表 1　区块链可扩展性问题模型归纳

区块链扩展技术路线	问题模型
网络层扩展	如何优化区块链的底层信息传递网络
链上层扩展	如何优化区块大小、节点组织、共识机制及区块链结构
链下层扩展	如何优化区块链在频繁交易、复杂计算和多链联合等场景应用

网络扩展不改变区块链的架构, 保留区块链的原有运行规则, 利用底层中继网络或对 OSI 模型底层进行优化, 进而提升区块链性能.

链上扩展主要改进区块链的数据层、网络层、共识层以及激励层, 对区块链区块结构、链结构、共识算法和网络模型进行优化, 通过优化完善区块链自身体系结构来提升其性能.

链下扩展针对区块链的合约层和应用层, 为了减少区块链的负担将复杂的计算或交易放到链外进行, 通过优化区块链外联能力来解决可扩展性.

3.1　网络拓展

区块链网络扩展是对 OSI 模型中的物理层、数据链路层、网络层、传输层进行优化. 包括对中继网络和分发网络的优化、对 OSI 模型的优化、对信息传播协议的优化.

3.1.1　中继网络和分发网络

2016 年, 基于传统中继网络思想, 比特币核心开发者 Matt 提出比特币中继网络 (bitcoin relay network, BRN)[15]. 该网络在全球范围内利用亚马逊服务器搭建中继网络节点, 与大多数矿工和矿池相连, 可以减少区块链共识和传播的延迟, 将区块数据快速的分发给网络中的其他节点. 2019 年 Matt 提出了一种基于用户数据报协议 (user datagram protocol, UDP) 的中继网络, 称为高速互联网比特币中继引擎 (fast internet bitcoin relay engine, FIBRE)[16], 可以在网

络节点间中继传输区块, 还利用区块压缩策略减少数据传输, 进一步优化区块传输的网络延迟. 康奈尔大学的 Soumya 提出另一个中继网络 Falcon[17], 其主要特点是用直通路由代替存储转发, 接收到区块的部分时就进行传播而无需等待接收到一个完整的区块, 可以减少网络传输延迟.

内容分发网络 (content delivery network, CDN) 的主要思想是借助距离用户最近的服务器将网络内容更快、更可靠地进行发送. bloXroute[18]将 CDN 的思想应用于区块链, 实现区块链分发网络 (blockchain distribute network, BDN), 从优化网络传输方面提高区块链可扩展性.

bloXroute 主要包含 4 个组成部分: 中继、网关、控制平面和区块链节点, 如图 2. 构成 BDN 的服务器称为中继, 包括交易中继和区块中继. 为区块链节点和 BDN 提供通信的软件称为网关, 可以比点对点网络 (peer to peer, P2P) 更快地向全节点传输区块和交易, 与网关相连的区块链全节点 (全节点指包含整个区块链完整历史事务信息的区块链节点) 认为网关是另外一个节点. 控制平面根据地理位置信息给连接 BDN 的网关提供最低延迟的中继服务列表. 网关本身不是全节点, 与全节点通信时无法验证区块, 因此需要部署一些区块链节点协助网关响应正常的区块链请求. 此外, bloXroute 使用直通路由技术以及区块压缩策略进一步提升性能.

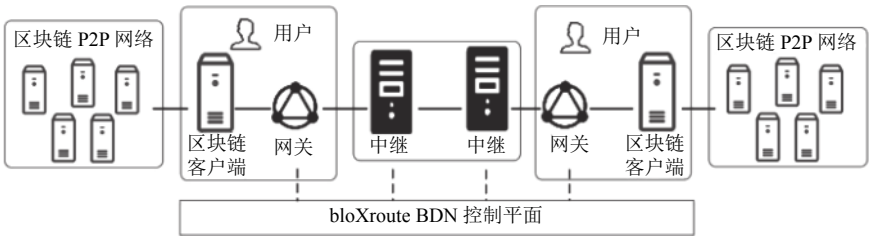

图 2 bloXroute 结构

3.1.2 优化 OSI 模型

单播通信和广播通信存在信息传播效率低的问题, 主要是因为它们采取的单方发送多方接收的传输方式, 组播通信允许一个或多个信息源同时对不同用户发送单一数据包, 有效地解决上述问题, 提高网络传播效率. 区块链项目 Nexus[19]应用组播通信技术, 关键思想是在网络层通过自设寻址协议连通局域网内外节点, 并利用 IP 组播技术实现底层数据包广播, 处理网络层而不是应用层上的包复制, 极大地加快传播速度.

2013 年, Google 基于 UDP 协议提出新一代多路并发网络传输协议, 即快速 UDP 互联网连接协议 (quick UDP Internet connection, QUIC)[20], 区块链项目 Harmony[21]中采用了该协议. Harmony 进行多方面的优化提高区块链的可扩展性. 在上层设计中, Harmony 采用分片技术, 分片内通过实用拜占庭容错算法 (practical Byzantine fault tolerance, PBFT) 快速达成共识. 在 OSI 的网络层, Harmony 使用 QUIC 减少底层数据包交换次数, 更快速且安全地传输消息. 除此之外, Harmony 利用专门的库操作系统构建的单地址空间机器镜像, 进一步扩展单个节点的性能.

3.1.3 改进信息传播

还有一些方案针对区块链网络中信息传播设计协议, 优化交易和区块的传播, 也属于底层扩展方案. Erlay[22]是一个优化交易传播协议, 可以将节点所消耗的带宽节省 40%. 允许以较小的成本建立更多的连接来提高网络的安全性, 并通过加强网络的抗攻击性来提高隐私性. 它以非常少的带宽和延迟成本有效地增加了网络连接. Velocity[23]利用一种叫无码率抹除码 (Fountain) 的技术来减少数据的传播量, 相同时间可以传输更多的信息, 改进区块传播, 提高交易吞吐量. Kadcast[24]是一种快速、安全、高效的区块传播协议, 其采取的 P2P 重叠网络传输协议 (Kademlia) 是一种著名的结构化覆盖拓扑结构, 用于高效的广播操作, 具有可调节的冗余和开销. Compact-Blocks[25]和 Xtreme Thinblocks[26]等区块压缩方案也关注区块传播的优化.

3.1.4 网络扩展技术总结

表 2 对底层扩展技术进行比较, 底层扩展技术不改变区块链自身的属性, 也不影响区块链的运行规则, 主要优

化物理网络中对于区块链数据的传播速度, 因此理论上这类方案对区块链的可扩展性的提升是最直接的. 但是, 这类解决方案的实际使用场景有限, 主要体现在以下几点.

(1) 中继网络和分发网络并不是 P2P 网络的代替, 而是为特殊需求提供节点间连接的覆盖网络.

(2) 中继网络和分发网络的方案都需要搭建高性能的底层通信网络, 成本很高.

(3) 限制区块链可扩展性的主要因素是区块链本身的属性, 因此这类方案提升效果有限.

表 2　网络扩展方案对比

扩展方案	扩展技术	应用场景	非中心化	优点	缺点
FIBRE[16]	中继网络	特殊	需要特殊中继节点 (较差)	不可感知性 可与上层扩展兼容	实现成本较大
bloXroute[18]	分发网络	特殊	需要特殊全节点 (较差)	不可感知性 不影响区块链运行机制	技术不成熟 实现成本较大
Nexus[19]	优化OSI模型	任意	利用组播通信 (较好)	优化数据处理 可与上层扩展兼容	可扩展性的提升有限
Erlay[22]	改进信息传播	任意	优化交易传播协议 (较好)	节约开销 具有一定隐私性	未对区块传输优化 可扩展性的提升有限

底层扩展技术关注度较低, 但要做到对区块链可扩展性的大幅突破必须全面考量, 针对区块链信息传播协议的改进更是不可或缺的. 更快的区块传播可以实现更短的区块间隔或在相同区块间隔时传输更大的区块, 从而提高交易吞吐量. 因此, 优化区块链中数据传播的协议是未来区块链系统增强可扩展性的途径之一. 目前区块链系统的传播协议仍有很大的优化空间, 比如更好的路由机制将有助于提高区块链的可扩展性.

3.2　链上扩展

区块链系统包含很多方面的设计工作, 如区块的数据结构、链结构和密码协议的设计、P2P 网络的构建、区块的传播和验证以及共识机制和激励机制等. 这些设计对应着区块链模型的 1–4 层, 代表着区块链的基本属性. 对这些设计的优化和改进是提高区块链可扩展性的重要途径.

不同的解决方案关注点不一样, 对于区块链模型不同层级的优化也各有偏向, 将这些方案最具特色的点作为分类的依据, 链上扩展技术方案可细分为优化区块数据、分片、共识协议改进和新型链结构 4 个子类. 优化区块数据主要涉及数据层优化, 共识协议改进主要对区块链共识层进行改进, 分片主要针对区块链网络层, 新型链结构涉及数据层和共识层等. 激励层主要作用是鼓励矿工产生区块和交易, 有助于区块链平稳向前推进, 其并不直接影响可扩展性.

3.2.1　优化区块数据

区块是区块链的基本组成单位, 区块的主要数据内容是交易. TPS 是衡量区块链可扩展性的重要指标, 所以区块的数据的优化和区块链可扩展性提升有着直接的关联. 显然, 增加区块的大小可以包含更多的交易, 进而提高交易吞吐量, 区块压缩也可以起到相同的作用. 几种主要的区块数据优化技术如下.

(1) 扩块

在区块链系统中, 区块的大小是有限制的, 最初中本聪规定的比特币区块大小不超过 1 MB. 扩块的基本思想是不改变区块的生成间隔, 增加区块的大小, 进而提高区块链的交易吞吐量. 2016 年, Croman 等人[27]报告称, 比特币在区块间隔平均为 10 min 的前提下, 区块最大不应该超过 4 MB, 相应的最大吞吐量为 27 TPS. 比特币现金 (bitcoin cash)[28]将区块扩大到 8 MB, 之后扩展到 32 MB, 可以直观地提高交易吞吐量. 但是直接扩大区块会增大传播延迟引发安全威胁, 比如导致分叉可能性增大和 DoS 攻击.

在区块链中, 为了保证交易的可验证并防止被篡改, 交易内容中包含用来验证该交易有效性的信息. 主要是由交易发起者提供的用来验证数字资产所有权以及可用性的数字签名, 这些数据占用整个交易存储空间近 65% 的容量. 因此通过缩减验证信息占用的空间来存储更多的交易, 可以获得更好的吞吐量, 这就是隔离见证 (segregated witness)[29]的出发点. 如图 3 所示, 隔离见证将见证信息 (签名数据) 从交易内容中解耦, 释放空间用以存储更多交

易数据. 交易数据仅包含交易发送者和接收者 (输入和输出), 1 MB 的空间可以存储更多的交易 (基础交易区块), 分离出来的见证数据放到区块的末尾 (扩充区块). 隔离见证可以有效提高区块的容量, 修复交易延展性, 但是会导致硬分叉问题, 而且对于可扩展性的提升效果有限, 大约是 17–23 TPS.

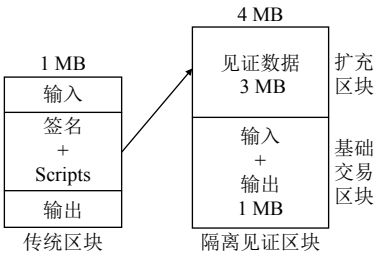

图 3 隔离见证

(2) 区块压缩

区块压缩的核心思想是尽可能地减少区块中的冗余数据, 如已经存储在验证节点交易池中的数据, 具有代表性的方案有致密区块中继 (compact block relay)[30]. 不同于比特币, compact block relay 只广播压缩区块, 压缩区块不需要存储完整的交易数据. 压缩区块主要由区块头和交易 ID 的短哈希值组成, 交易 ID 的短哈希值将用于匹配已经存在于验证节点交易池中的交易. 收到压缩区块的节点验证交易缓存池是否包含压缩区块中的每笔交易. 如果交易都在缓存池中, 则可以重新构造出完整的区块; 如果有不存在的交易, 向发送区块的节点请求发送缺少的交易. 加盐短哈希有损区块压缩算法 (Txilm) 在 compact block relay 基础上进行了改进, 将 compact block relay 区块中每个 TX 表示的大小减小到约 40 比特, 提高了区块被压缩的程度, 利用交易规范排序 (canonical transaction ordering rule, CTOR) 的规则计算哈希值以降低压缩后 TXID 冲突的概率, 并利用循环冗余算法 CRC32-merkle 根作为盐, 对 TXID 进行哈希加盐来防止遭受碰撞攻击.

3.2.2 分 片

分片最初是数据库领域的一种分区技术, 如图 4 所示, 主要思想是分而治之, 将一个大型数据库分割成较小的片区, 并存储在不同的服务器上, 使其能够更快、更高效地管理数据. 2016 年, Luu 等人第 1 次在区块链领域提出了分片的概念, 即 Elastico 协议[31]. 核心思想是将一个区块链网络划分为若干个较小的网络, 每个小的网络称为一个分片, 每个分片包含一部分区块链节点. 采用分片技术来提高可扩展性的方案还有 OmniLedger[32]、RapidChain[33]、Monoxide[34]、ByShard[35]、AHL[36]、SharPer[37]、Meepo[38]等, 表 3 对这些方案进行了比较. 其中同步网络中所有信息都可以在已知的时间间隔内到达, 部分同步网络中所有信息可以在未知的时间间隔内到达, 异步网络不保证所有的信息可以到达.

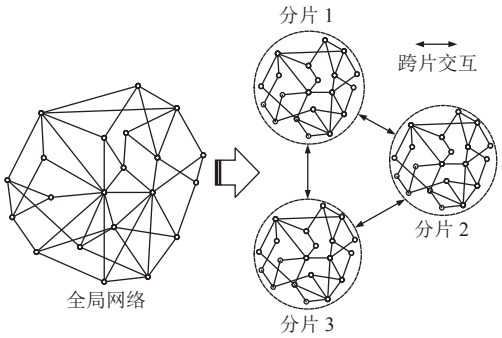

图 4 分片

Elastico 按照轮次执行, 每轮通过 PoW 将全网节点划分为 1 个目录分片和 16 个普通分片 (上限为 100 个). 目录分片为后续节点提供分片分配和分片成员身份列表服务. 每个普通分片不超过 100 个节点, 普通分片内部通过 PBFT 产生区块. 不同的普通分片并行处理交易, 提高交易提交和验证的效率, 从而提高整个网络的吞吐量.

Elastico 通过将每个普通分片产生的区块合并为一个区块加入区块链, 可将吞吐量提高到 40 TPS. 然而节点的加入和退出导致频繁的节点分片分配和分片成员更新, 严重限制了区块链性能. Elastico 每个节点都需要存储区块链数据限制了其可扩展性. 由于采用 PBFT 协议以及分配到每个片区成员很少, Elastico 只能容忍 25% 的恶意节点. 并且, 由于跨片交易需要通过目录分片查询对应用户所在的分片, 产生了额外的确认延迟. Elastico 没有跨片交易原子性, 可能发生跨片交易错误.

表 3　分片方案比较

属性	Elastico[31]	OmniLedger[32]	RapidChain[33]	Monixide[34]	ByShard[35]	AHL[36]
出块共识	PBFT	ByzCoinX	50%BFT	PoW	PBFT	PBFT
片区划分	PoW	PBFT/PoW	PoS	固定	固定	Intel SGX
分片规模	<100	<64	<256	2048	<64	<12
单片大小	<100	2^2–2^{10}	3–256	24	<100	<33
吞吐量 (TPS)	40	3500	7380	11694	5000	2000
延迟 (s)	<900	800	8.7	23	4	2
片内安全性 (%)	25	25	33	50	25	25
整体安全性 (%)	33	33	50	50	33	33
网络同步	部分同步	部分同步	部分同步	异步	部分同步	部分同步

OmniLedger 协议提出一种实时的分片间交易方案, 在片区划分时采取无偏差随机函数, 使得 OmniLedger 抗偏置性强于 Elastico. 由于采用了公开可验证秘密分享, 使得验证者能够安全且有效地验证节点随机数的正确性. 虽然 OmniLedger 也需要少量的主要成员, 但是其 ByzcoinX 共识机制可以通过一个固定高度的树结构结合 PBFT 和 PoW. 得益于此, OmniLedger 有 3 个分片 (上限为 64), 每个分片有 600 个节点 (上限为 1024), 可以达到 3500 TPS 的吞吐量, 延迟在 800 s 左右. OmniLedger 具备不低于 Elastico 的安全性并且延迟更小. OmniLedger 介绍了一种双阶段保证跨分片交易原子性的方法, 在跨分片交易处理过程中, 第 1 阶段先在本分片锁定该交易, 然后在目标分片中启动第 2 阶段解锁该交易, 使得两阶段要么都成功, 要么都失败, 保证了一致性. 但是 OmniLedger 在跨片交易处理时轻量级节点受到限制. 而且初始的随机性依赖于第三方, 这使得 OmniLedger 在网络同步时受限.

RapidChain 实现了不需要经过可信的初始化设置就能进行分片, 可以在全网实现 33% 的容忍能力, 片内可以做到 50% 的容忍度. RapidChain 使用一个快速的跨片交互协议, 不需要将交易传播到全网. 利用可视秘密共享 (visual secret sharing, VSS) 实现无偏差随机性, 基于此实现片内快速出块, 提高了吞吐量和可扩展性. RapidChain 在 4000 个节点的网络可以实现 7300 TPS 的吞吐量和 8.7 s 的延迟. 然而, Rappid 使用的 BFT 共识只适用于小规模的分片, 增大分片规模会导致交互开销过大.

Monixide 使用 PoW 的变体作为其出块共识, 通过异步的方式做到对区块链的线性扩展. 分片之间平行地处理内部交易, 而不需要和其余分片交互, 并且其跨分片交易具备最终原子性. Monixide 基于合并挖矿提出诸葛连弩挖矿机制, 实现矿工可以在多个分片同时挖矿, 所以分片内的算力接近于全网算力, 因此片内的安全性和全网安全性一致. 在 48000 个节点设定下, Monixide 的吞吐量可达到 11694 TPS, 延迟在 13–21 s. 然而, Monixide 对于节点的性能要求很高, 并且较高的复杂度可能会引入中心节点导致中心化问题.

在联盟链中, 也有一些优秀的分片方案. ByShard 为联盟链分片协议制定了框架. AHL 该方案将节点随机分配到每个分片, 为了在保证安全性的前提下减少每个分片的节点, 可信的硬件 Intel SGX 来限制节点的恶意行为, 从而可以在每个分片节点数量较少的情况下保证分片的安全. 对于跨分片事务, AHL 通过一组额外的节点来进行处理. SharPer 是另一个联盟链的分片方案, 该系统由一组容错集群组成, 每个集群维护区块链账本的一个分片. 这些集群分别处理内部事务, 并且这些集群互相有重叠部分, 当遇到跨分片共识后, 就在重叠部分进行共识.

Meepo 也是一个基于联盟区块链系统的分片方案. 它使用每个区块共识结束后进行跨分片通信的协议实现高效有序的跨分片通信. 此外, 它设计了一种部分交叉调用合并策略, 这种策略支持将不同分片智能合约调用整合到每一个分片内. 它还设置了重放时间, 一旦发生事务异常, 在重放时间内重新执行正确的事务, 恢复错误的事务, 保

证跨分片交易的原子性. 最后 Meepo 添加影子碎片作为碎片的备份, 一旦任何碎片关闭, 联盟成员可以切换到相应的备份, 以继续执行区块链交易, 显著降低了单点故障对系统可用性的影响.

3.2.3 共识协议

区块链的共识协议促使区块链成员对于区块链状态更新形成共识, 保持一致性. 已经用于区块链的共识机制有 PoW、权益证明共识机制 (PoS)、PBFT 等, 然而早期的共识协议无法满足可扩展性需求, 本节介绍基于这些经典共识机制的改进方案, 它们对于提高区块链可扩展性有重要意义. 利用选取出块节点的确定性将共识协议分为概率性共识和非概率性共识两类, 概率性共识是在出块前全网没有达成一致, 后期根据最长链原则等对块达成高概率的共识, 主要包含基于 PoW 和 PoS 机制的协议; 非概率性共识是在出块前全网对该块达成一致, 主要包含 PBFT 和混合共识协议.

(1) 概率性共识

PoW 能够保证较强的安全性, 许多研究优化最初的中本聪协议的以提高可扩展性, 优化主要包含分离设计、更换主链选取原则、降低挖矿难度几个方面.

首先, 中本聪协议吞吐量低的一个原因是区块提交和交易打包不能并行, 例如在比特币中矿工需要先打包交易, 然后所有矿工一起通过 PoW 竞争区块提交权, 在选出区块提交者之前无法继续打包交易. 因此, 有研究者提出将 PoW 计算和交易打包分离的思想, 如 Bitcoin-NG[39].

Bitcoin-NG 将交易打包和领导选举的 PoW 计算分离. 原理如图 5 所示, Bitcoin-NG 包含主区块和微区块两种类型的区块. 主区块通过 PoW 计算竞争记账权力, 即参与领导选举, 主区块包含用于验证微区块所属权的公钥, 不涉及交易相关数据. 微区块不需要进行 PoW 计算, 只需按照设定好的速率产生并连接到前一个主区块或微区块. 区块链成员在生成微区块时需要包含与主区块包含的公钥相匹配的私钥签名, 其他的区块链成员收到主区块后进行 PoW 验证, 收到微区块后验证其签名是否匹配最新主区块公钥. Bitcoin-NG 将 PoW 证明和交易打包分离, 区块链成员可以通过生成微区块的方式扩大吞吐量. 但是, 这类设计会存在局部中心化威胁, 当攻击者产生主区块时, 他在一定时间段内对区块链的状态更新具有控制权.

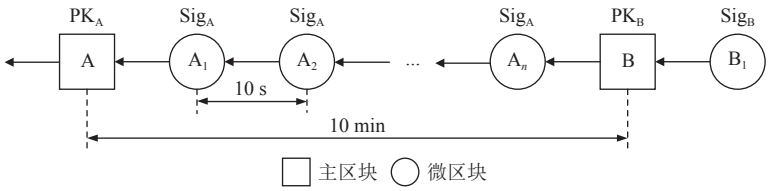

图 5 Bitcoin-NG 结构

此外, 严格的最长链原则是限制中本聪协议可扩展性的另一个原因. 每次挖矿竞争中会有很多区块链成员进行大量的计算但未能产生满足难度值要求的区块或者产生有分歧的区块, 最终只会保留一条主链, 不在主链上的区块都会作废. 因此, 有研究提出改变主链选取原则和降低挖矿难度值的方案.

为了优化主链选取规则, 有研究提出新的主链选择方法贪婪最重可观测子树算法 (greedy heaviest-observed sub-tree, GHOST)[40]. 该协议选择包含子树最多的链作为主链而不是选择最长的链. 在一定程度上缓解攻击者针对最长链进行分叉的风险, 提高区块链吞吐量.

为了使更多的区块可以包含到区块链系统, 有研究者提出降低出块难度阈值来减小出块间隔的想法, 也被称为弱解方案. Subchains[41]给出理论上的弱解设计: 当区块链成员在进行 PoW 计算时如果满足弱解难度值, 则生成弱区块; 当区块链成员 PoW 计算满足强解难度值时, 生成强区块. 由于相邻两个强区块之间的弱区块是顺序生成的, 并且生成的难度值低, 所以恶意敌手可以通过隐藏若区块形成非法弱解链, 所以 Subchains 存在着针对弱解链的自私挖矿问题. 自私挖矿是恶意区块链成员产生区块却不发布, 进而对系统造成威胁的一种攻击. FruitChains[42]划分两个挖矿难度值分别用于产生两种存储交易的数据结构如图 6 所示, 高难度值用于产生区块, 低难度值用于产生弱解区块, 称为水果. 区块可以包含与其高度值相近的水果, 区块链成员产生水果或区块都可以获得奖励, 区

块包含水果也可以获得收益. 最终的交易账本是由区块构成的链决定. FruitChains 不直接将弱解区块作为最终账本, 可以缓解自私挖矿问题, 但是会有不同的区块重复引用相同水果的问题, 占用大量存储资源. FruitChains 使得更多的交易通过水果加入到区块链系统, 提高了交易吞吐量.

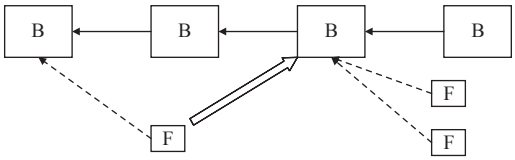

图 6　FruitChains 的弱解方案

PoS 中的区块链成员不需要消耗计算资源生成区块, 而是通过用户在区块链系统中的资产作为投票权重, 对每个节点来投票选举领本次共识的导者, 从而节约计算资源并减少交易的确认时间. PoS 的理念是系统中拥有更多权益货币的区块链成员不太可能对系统造成威胁. 改进的 PoS 算法有 Ouroboros[43], 在 PoS 中一个节点被选中出块的概率和其拥有的权益占比相关. Ouroboros 强调选择过程的随机性, 采用简单随机数算法 (coin-tossing) 选举当前时段的领导者和下一个时段的随机种子, 并利用可验证秘密共享[44]将生成的随机数分发给参与者. PoS 主要通过利用权益证明代替计算证明的方式加快出块间隔, 提高共识速度, 进而提高区块链的吞吐量.

雪崩链协议采用了全新的共识机制 Avalanche, 该共识机制的做法是在既有的数百个以至更多节点当中, 以快速而多次的抽样方式获得多次验证结果, 只要某一结果多次在验证节点中得到超过半数节点的认同, 则该结果达成共识. Avalanche 中存在 3 条区块链, 交易链负责资产的建立与交易, 平台链负责存储和验证链上的数据, 合约链负责智能合约相关功能.

(2) 非概率性共识

PoW 和 PoS 都属于间接形成共识的机制, 通过竞争记账权来保证共识验证, 出块节点具有概率性. 分布式系统很早就提出了 PBFT. 由于具备较好的可扩展性和拜占庭容错, PBFT 被广泛地应用于私有链和联盟链. 然而, 因为其节点数量众多, 通信开销很大, 为 $O(n^2)$, 实际上 PBFT 更适用于较少节点的情况. 当节点数 $n=3\times f+1$ 时, PBFT 可以容忍 1/3 的恶意节点 $f=(n-1)/3$. PBFT 按照轮次执行, 每一轮参与节点包含主节点和备份节点, 当每一轮共识开始时, 随机选取备份节点作为主节点. 主节点可以决定 3 阶段 (预备、准备、确认) 交互过程的结果, 判定一个区块被同意加入到链还是被拒绝. HyperLedger Fabric 使用 PBFT 达到超过 1 000 TPS 的吞吐量.

一些方案对 PBFT 进行改进以获得更好的可扩展性和处理大量节点问题. 例如, Dumbo[45]通过分组来减少 PBFT 共识所需的节点数量. 少量的节点在通信时的复杂度会降低, 有助于提高吞吐量.

Hot-Stuff[46]共识协议由 Yin 等人提出, 它对 PBFT 做出改进. 其采用并行流水线处理提议, 相当于将 PBFT 中的后一轮的准备和前一轮承诺阶段的两个广播合并成一个广播, 很大程度上提升了共识的效率. 该协议利用门限签名技术将领导者作为签名验证者, 使得每次信息确认只需要每个节点将签名发送给领导者, 而不用全网广播, 这降低了通信复杂度.

一些方案通过事先对事物顺序进行确定性排序, 消除了共识中对事物顺序排序的共识步骤, 增加了区块链系统的性能, 例如 NeuChain[47]通过专门的事物编号分配服务器对事物进行编号分配, 从而提高了整体的共识效率.

在共识协议中, 也有一些场景需要共识协议保护数据的隐私. Caper[48]共识协议针对企业内部隐私保护需求的场景, 每个参与者维护私有数据和公共数据, 每个企业只访问和维护自己的账本视图, 这包括其内部和所有跨企业事务. 系统支持内部和跨企业交易, 其中内部交易由单个企业执行, 而跨企业交易由所有企业执行. Qanaat[49]在 Caper 的基础上进行了扩展, 将单个企业内的隐私数据保护扩展到了企业之间的隐私数据保护.

还有一些非概率性共识通过对网络进行分层, 分层后每个层级的节点在本层内共识, 这减少了全局通信, 降低了通信复杂度, 代表方案有 Steward, Blockplane[50], GEOBFT. 其中 Blockplane 以地理位置为依据进行分层, 属于同一个地理位置的节点进行内部共识, 这减少了全局通信, 并且这种分层设计可以预防地质灾害对整个系统的影响.

混合共识是一种结合多种共识协议提高可扩展性的共识方法. ByzCoin[51]基于 Bitcoin-NG[39]的思想提出一个两阶段协议, 通过结合 PoW 和 PBFT 来保证强一致性, 和 Bitcoin-NG 类似的分离设计提高区块链的交易吞吐量. 使用一个树结构交互模式在准备和提交阶段进一步改进 PBFT, 实现确认延迟在 15–20 s 并且吞吐量超过 1 500 TPS. Hybrid consensus、Solidus 也提出将不同的共识协议与 PoW 相结合, 采取相似的交易分离思想和两阶段的混合共识算法.

3.2.4 新型链结构

上述方案大多采用单一链结构, 对于吞吐量的提升具有局限性, 有研究提出改变链结构来组织区块, 可进一步改善可扩展性. 主要分为有向无环图结构 (directed acyclic graph, DAG) 和平行结构.

(1) 有向无环图

传统的区块链的单一链结构存在孤块问题[52], 即分叉后一段时间, 只有在主链上的区块能够被确认, 不在最长链的区块作废, 这限制了区块链系统的吞吐量. 为了解决这个问题, 有研究提出将有向无环图 DAG 应用于区块链. 直观的做法是让区块作为 DAG 中的顶点, 区块间的关系作为边, 将链状结构的区块链转化为 DAG 结构. 允许多个顶点连接到之前的顶点, 这意味着区块可以并发地生成, 有效地解决链式结构区块分歧的问题, 从而使得区块链系统可以包含更多的交易. 采用 DAG 结构的可扩展性方案发展迅速, 本文根据链结构增长的表现形式将 DAG 结构分为发散结构和收敛结构.

发散 DAG 结构方案有 Spectre 和 Phantom 等. Spectre 可以指定 DAG 结构中两两区块间的局部顺序, 但是不能提供完整交易列表. Spectre 的关键技术是基于底层拓扑排序中区块的优先级提出一个递归的权重投票算法, 如图 7 所示. 新加入的区块需要为之前的一对区块 (x,y) 进行先后关系投票, 投票存在 3 种选择 (−1, 0, 1), 表示两个区块的先后关系 $(x<y, x=y, x>y)$. 最终该区块对 (x,y) 的先后关系由该区块总计的投票结果的绝对值决定. 这个设计需要假设任意两个交易的顺序一定是由诚实节点得到的, 因此 Spectre 的区块更新缓慢.

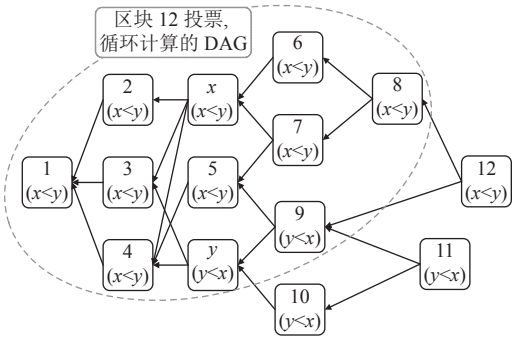

图 7 发散的 DAG 结构 (Spectre)

Phantom 的每个区块包含多个哈希引用指向之前的区块, 也被多个后续区块引用. 首先标识一组连接良好的区块, 进而大概率排除非诚实节点产生的区块. 之后, Phantom 利用一个递归的贪婪算法, 实现对标识区块的排序. 贪婪算法通过迭代不断地激励拓扑中被标识的区块并惩罚其余的区块. 变化参数来调节并发区块中的容忍度. 区块排序后可以进行交易排序, 最终全网达成一致状态. 与 Spectre 类似, Phantom 也依赖于诚实节点来对区块进行排序, 但是 Phantom 可以确保全局区块有一个严格的线性顺序.

收敛 DAG 结构的扩展方案有 Inclusive[53]和 Conflux[54]等. 在 Inclusive 中, 新区块通过哈希引用指向多个之前的区块. 提出了一种新的包容性方案在 DAG 结构中选取主链, 而不是普通区块链的最长链原则. Inclusive 可以包容多个并发区块中冲突的交易, 有助于提高吞吐量和对大区块的传播延迟的容忍性. Conflux 提出两种不同的区块之间的连接, 父连接和参考连接, 在确定主链的基础上, 新生成的区块必须使用父连接连接到主链的最后一个区块上. 除了主链外, 还存在其他一些非主链的链, 新生成的区块必须使用参考链接连接这些非主链的最后一个区块, 最终通过选择算法选择由父连接构成的链作为主链, 如图 8 所示. 在区块确认时 Conflux 将 DAG 的共识问题转化

为单链结构的共识问题, 采用 GHOST 来解决主链选取问题. Conflux 实现了 6400 TPS 的吞吐量, 延迟在 250–450 s.

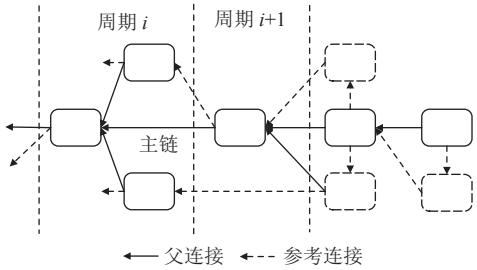

图 8　收敛的 DAG 结构 (Conflux)

DAG-Rider 是基于拜占庭共识的异步原子广播协议, 它依靠可靠广播来保证所有参与的节点最终都能看到相同的 DAG. DAG-Rider 分为两层, 在第 1 层中, 各个节点通过可靠广播发送事务, 并构建他们之间通信的结构化 DAG. 在第 2 层中, 各个节点观察本地存储的 DAG, 并在没有额外沟通的情况下对所有提案进行完全排序, 具有高弹性、低时间复杂度的优点.

IOTA 将交易排序成 DAG 图, 也属于 DAG 链结构. 该共识方案中当一个人试图在 IOTA 系统增加一个交易, 需要随机找到其他两个没有确认的交易, 验证其有效性, 随后把你的交易指向这两笔交易, 会发送到网络, 由后来的交易检查和确认. 这种共识方式使得整个网络的规模越大, 效率越高.

(2) 平行结构

DAG 结构的一个缺点是无结构性, 近年来一些研究提出更具结构性的平行结构. 核心思想是借助平行结构并行产生区块, 此思想启发于比特币骨干协议的 2-for-1 PoW 挖矿思想. 2018 年, ParallelChain[55]提出形式化定义的 m-for-1 平行链链协议, 它对于 PoS 和 PoW 分别进行了扩展的概念设计, 提出了扩展单一链结构为多条平行链的做法, 并且其相较于 DAG 结构更加易于维持时序性. 此外, 已有的平行结构的扩展方案还有 OHIE[56]和 Prism[57]等.

OHIE 是对 ParallelChain 的 PoW 部分的模型进行了实际设计如图 9 所示. 将前置多个区块的哈希计算默克尔树哈希作为前置状态, 利用哈希值中特定的几位的数值对新产生的区块进行定位. 将单条链结构扩展为多条链并行的结构, 缓解区块分歧的问题, 提高交易吞吐量. Prism 的主要思想是对区块链进行功能解构, 将之前单一的区块分为交易区块、提交区块和投票区块这 3 种类型. 交易区块负责打包交易, 提高区块链的高吞吐量, 提交区块和投票区块构成平行结构. 提交区块负责引用交易区块, 完成交易的上链, 投票区块对提交区块进行投票, 减少区块的确认延迟.

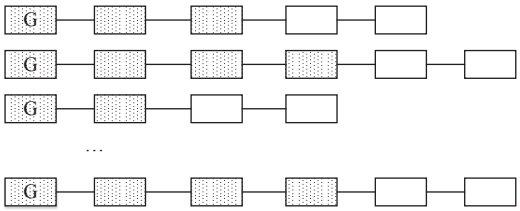

图 9　平行结构 (OHIE)

3.2.5　链上扩展技术总结

链上扩展技术针对区块链本身的设计进行优化和改进, 以提高区块链的交易吞吐量, 解决可扩展性问题. 这类技术可以从区块链架构的基础设计出发改善区块链自身的属性. 本节对链上扩展技术的各个子类进行比较, 在表 3 中给出了比较结果.

对于共识协议, 链上扩展的方案多采用单一的共识机制, 分片技术和混合共识方案会采用两种以上的共识方

法. 分片在委员会 (主片区) 成员选取时和片内产生区块时会采用不同的机制, 混合共识机制大多是为了进一步提高吞吐量而设计领导节点选举方法而加快出块以提高吞吐量.

在端到端性能方面, 分片、非概率性共识和新型链结构均能达到 10^3 数量级的吞吐量, 延迟均不超过中本聪协议. 分片不需要实时在全网同步状态加速区块处理, 可以有效地提高吞吐量, 但实际多个分片间信息交互需要一定的开销. 非概率性共识可以极大程度减少区块分歧, 在保证吞吐量的同时延迟非常低, 但这类方案往往需要中心化的设施. 新型链结构实现了区块的并发大幅改善吞吐量, 延迟方面多数方案沿用中本聪协议的设计.

链上扩展的安全性主要考虑容忍恶意节点的比例以及对于双花攻击的抵御能力. 对恶意节点的容忍能力和共识机制直接相关, 采取 PoW 或者 PoS 的方案安全性相对较高, 通常可容忍 51% 的恶意节点. 但是 Bitcoin-NG 的微区块设计可能会导致攻击者可以更容易干扰区块链状态, 故其对于恶意攻击者的抗性较低. 此外, 对于分片方案需要考虑片内安全性和整体安全性, 取片内安全性作为衡量指标, 主要原因是网络被分区, 每个区域的节点数量变少, 恶意节点更容易针对片区进行攻击.

链上扩展方案大多数具备良好的中心化, 因为多数区块链协议在底层基础设计时以公有链为出发点. 但也有部分非概率性方案以私有链和联盟链的场景为主, 他们往往需要许可环境建立信任机制. 此外, 一些分片方案和 DAG 结构也可能需要中心化设计, 比如分片的委员会由可信的成员节点构建, DAG 在主链选取时必须假设节点必须被信任等. 表 4 中, ◐指的是这些方案设计了特殊的委员会, 所以存在一定程度的中心化; ○指的是这些方案设计了特殊领导节点, 所以存在很大程度的中心化; ●指的是这些方案没有设计特殊节点, 所以中心化程度低.

表 4 链上扩展方案对比

方案	技术	吞吐量 (TPS)	延迟 (s)	安全参数 (%)	双花攻击	非中心化	成本
Bitcoin Cash[28]	优化区块	60	600	51	√	●	低
Compact Block Relay[30]		N/A	N/A	51	√	●	低
OmniLedger[32]	分片	3 500	800	25	√	◐	高
Elastico[31]		40	<900	33	√	◐	高
RapidChain[33]		7 380	8.7	50	√	◐	高
Monixide[34]		11 694	23	50	√	◐	高
ByShard[35]		5 000	4	33	√	◐	高
AHL[36]		2 000	2	33	√	◐	高
Bitcoin-NG[39]	修改共识	100	10–600	25	√	●	低
FruitChains[42]		N/A	N/A	51	√	●	低
Ouroboros[43]		260	120	51	√	●	低
Dumbo[45]		18 000	24	33	√	○	低
HotStuff[46]		20 000	0.08	33	√	○	低
HyperLedger Fabric[9]		1 500	N/A	33	√	○	低
Byzcoin[51]		1 000	15–20	25	√	●	中
Conflux[54]	修改链结构	6 400	250–450	51	×	◐	中
OHIE[56]		2 400	200–600	51	√	●	低

此外, 链上扩展的成本指标主要考虑协议实现难度和系统实施成本, 多数链上扩展方案协议复杂度并不是很高, 而且方案实施不需要特别多的实体, 因此成本较低. 一些 DAG 方案在实现时由于无法沿用传统单链的安全性, 需要较多的额外的开销来进行区块的时序处理. 一些混合共识和分片的方案在实现时往往对于参与节点的性能和网络的通信能力有一定的要求.

3.3 链下扩展

链下扩展是解决可扩展性问题的另一个选择, 这类方案建立在区块链的应用层和合约层, 可以在不改变区块链本身设计的基础上, 提高区块链的吞吐量. 举一个例子, 把区块链比作道路的话, 链内扩展相当于对道路进行交

通优化、车辆优化或者道路扩展等, 而链外扩展相当于不改变原本道路情况下增加隧道、铺设高架等. 这类方案利用区块链上层应用设计和智能合约将复杂的计算和频繁的交易迁移到区块链系统之外进行. 这类技术从两个角度实现区块链功能扩展, 一是将大部分交易或计算放到链下进行, 将结果返回给区块链, 也就是状态通道技术和链下计算技术, 极大地加快了交易确认, 有效地提高系统整体的交易吞吐量. 其次, 借助高性能辅助区块链提高可扩展性或者实现多个区块链系统交互联合, 也就是侧链技术和跨链技术.

3.3.1 状态通道

状态通道是一种临时性的链下交易通道, 将部分交易转移到这个通道上, 以达到减少主链交易量的效果, 同时提高整个系统的交易吞吐量. 主要思想是交易双方在区块链上建立临时的链下对等交易通道, 交易结束或到达预设的截止时间, 或者交易的任何一方将初始交易和最终交易的数据同步到区块链, 都表示交易通道关闭. 状态通道的机制相当于在链下提前对事务和交易进行了确认, 从而加快了区块的确认过程, 进而提高区块链的可扩展性. 主要的方案有闪电网络[58]、雷电网络[59]等支付通道以及 Trinity[60]、μRaiden[61]等扩展以太坊的状态通道.

闪电网络的支付网络是由多条链下支付通道组成的, 可以提高区块链的交易吞吐量. 交易双方通过哈希时间锁定合约 (hash time locked contract, HTLC) 创建支付通道如图 10 所示, 在通道内进行链下交易, 向区块链提交交易结果. 虽然建立支付通道的过程中涉及链上操作, 但通道内发生的所有交易都是链下的, 因此获得更高的交易吞吐量. 但是闪电网络也存在着一定缺陷: (1) 扩展交易但没有扩展用户; (2) 交易的安全性低于比特币; (3) 只适用于比特币的小型支付场景. 雷电网络设计思路和闪电网络类似, 是基于以太坊实现的, 而闪电网络是针对比特币网络的.

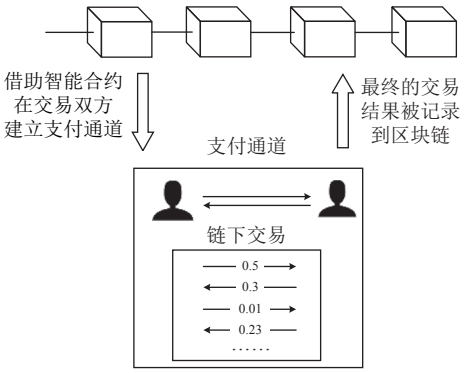

图 10 支付通道

Trinity 是一个通用的链下扩展解决方案, 具有实时支付、低交易费用、可扩展性和主链资产的隐私保护等特点. Trinity 包含 4 层架构: 通道服务层、通道网络层、状态通道层和区块层. 通道服务层为 Trinity 提供插件化、可定制的链下交易服务. 通道网络层为 Trinity 提供状态通道的路由服务, 该层为未建立状态通道的交易双方全自动智能选路. 状态通道层为 Trinity 提供最基础的 P2P 状态通道服务. 区块层是以 NEO 区块链为基础的主链. 通过使用状态通道, 交易吞吐量有效增加. 为了加强隐私保护, Trinity 采用零知识证明等多种技术来保护数据安全. 但是, Trinity 的使用场景受限于支付环境. μRaiden 是一个快速且免费的链外 ERC20 代币转换框架, 可用于基于两方基于 ERC20 代币的微型支付. 雷电网络旨在通过双向支付通道实现跨多个状态通道的资产转移, μRaiden 可以实现单向的支付通道. μRaiden 依赖以太坊本身的安全性, 收发双方基于自己的私钥和通道进行链上或者链下的交互, μRaiden 中的转账是免费的, 旨在打开和关闭支付通道时消耗费用. μRaiden 有助于发展以太坊的微支付功能, 但是它也从在一些缺点, 比如它不支持跨多个通道的交易, 只允许代币单向地发送给提前决定好的接收者.

3.3.2 链下计算

链下计算的主要思想是将原本在链上处理的计算和复杂交易放到链下处理, 链上仅作数据验证, 间接地提升

区块链处理数据的速度. 一个应用场景是, 以太坊的用户需要模拟所有合约的执行来验证其状态. 这个过程成本很高, 且限制了以太坊的可扩展性. 因此, 提出一些链下计算的方案来构建可扩展的智能合约, 即链下计算技术. 代表方案有 rollup[62]、TrueBit[63]、Arbitrum[64]、SlimChain[65]等.

针对以太坊的链下计算 rollup 方案, 该方案将以太坊中智能合约的计算 (以及状态存储) 转移至链下, 但将每笔事务的一些数据放在链上. 这种方案减轻了链上的计算存储负担, 又通过链上数据记录共识保证了安全性. rollup 方案的本质是将链上事务的执行放到链下执行, 并且在链上有一份智能合约记录链下事务执行的数据目前的状态, 即状态根. 链下事务执行后将许多事务压缩成一个汇总事务并记录该汇总事务执行前的旧状态根和执行后的新状态根, 再将该汇总事务上链, 所有链上节点接收到汇总事务之后, 不会执行汇总事务内的事务逻辑, 而只验证汇总事务, 智能合约检查提交的汇总事务的旧状态根是否匹配链上记录的目前的状态根, 如果匹配的话接受这些逻辑的执行结果, 智能合约对目前的状态根进行更新, 更新为新状态根. 根据链上节点如何验证汇总事务的正确性, rollup 方案可以分为 Optimistic rollup 与 ZK rollup. Optimistic rollup 方案中汇总事务提交者需进行资金担保, 当汇总事务提交后需要留一段时间给验证者来进行质疑, 验证者会追踪所有历史状态根, 并与提交的汇总事务的旧状态根进行比对, 如果发现历史状态根与汇总事务的旧状态根不匹配, 可以向区块链发送一个质疑证明, 证明该汇总事务不合法. 然后智能合约会根据链上存储的历史状态根信息和质疑证明进行计算, 经过判断后, 如果该事务非法, 则扣除提交者担保资金, 奖励验证者, 通过这种激励方式保证汇总事务正确性. ZK rollup 方案中在链下执行事务后, 通过零知识证明算法, 生成一个零知识证明和新状态根. 提交者将零知识证明与汇总事务一起上传到链上, 链上节点通过零知识证明验证旧状态根经过汇总事务执行之后会变成新状态根, 从而确保汇总事务正确性.在 ZK rollup 方案中, 不需要预留时间给验证者来进行质疑, 因为密码学保证了验算零知识证明就等价于验证了该汇总事务是合法的. 对比 Optimistic rollup 与 ZK rollup, Optimistic rollup 基于押金的安全性不是通过算法保证的, 并不是绝对安全的, 并且需要预留时间给验证者来进行质疑, 造成了资产从链下提到链上时需要被锁定一段时间, 这一点对于许多对及时性要求高的交易来说是不可接受的. ZK rollup 相对于上面这两点, 具有很大优势, 密码学算法保证了汇总事务的绝对安全合法, 而且不需要预留时间给验证者来进行质疑, 但是生成零知识证明比较复杂, 需要耗费算力和时间, 投入更高的硬件费用.

TrueBit[63]是由 Jason Teutsch 和 Solidity 语言的创造者 Christian Reitwiessner 在 2017 年推出的以太坊智能合约如, 旨在促进可信的计算密集型应用. 在以太坊主链上进行的计算代价很高, 因为交易是由网络上的所有完整节点同时处理的. 计算的补偿是以 gas 成本的形式给出的 (gas 是以太坊用于计算合约成本的度量单位). 每个区块都有一个最大的 gas 限制, 决定了一个区块中所有交易执行的计算总量上限. 因此, 复杂的计算难以包括在区块内. 如图 11 所示, TrueBit 将复杂的计算交给一个经过验证的第三方. 这个第三方被称为处理者, 它将代币存入智能合约, 所以是可信的. 另一个验证处理者工作的第三方被称为挑战者, 从验证工作中获取奖励. 挑战者可以识别导致分歧的操作. 因此, 以太坊的计算密集型工作减少了, 而且正确的结果也会被认可.

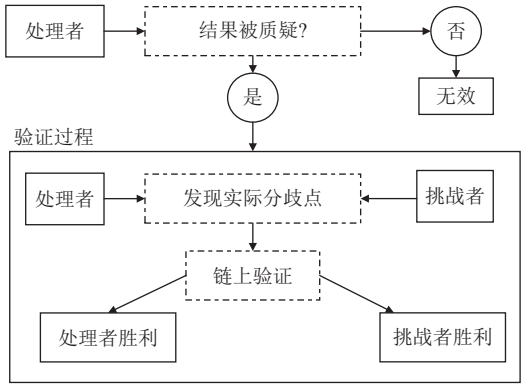

图 11 TrueBit 执行原理

Arbitrum 通过将智能合约的验证计算转移到链下进行, 可以提高吞吐量. 在 Arbitrum 中, 验证者验证全局的交易, 类似于比特币中的矿工. Arbitrum 利用一个虚拟机来实现一个带有资金的合约, 该合约的资金不会被任何执行透支. 任何参与方都可以创建一个虚拟机并选择一组管理者保证虚拟机正确执行. 如果所有的管理者同意更新虚拟机状态, 他们会签署一份无异议声明合约. 否则, 管理者签署一份有争议声明合约, 之后通过一个均等协议来处理虚拟机的状态变化. 这个方法和 TrueBit 类似, 为了保证虚拟机的状态正确变化. 管理者只需要验证代表合约状态的哈希值, 减轻了合约验证的负担, 有利于提高吞吐量.

SlimChain 是一个无状态区块链系统, 通过链外存储和并行处理来扩展交易. 其主要思想是利用链外存储节点来存储账本状态并模拟智能合约的执行. 链外存储节点并行执行链外交易, 并计算一些辅助信息, 以证明执行的完整性, 并促进链上共识节点的后续交易承诺. 然后, 它设计了链上临时状态, 这种状态提供了最少但足够的信息, 实现无状态链上事务验证、并发控制和承诺.

智能合约的状态是由验证者通过模仿所有合约的执行来验证的, 但验证的过程是昂贵的, 这降低了可扩展性. 链下计算技术将这些昂贵而复杂的计算在链外进行, 提高可扩展性.

3.3.3 侧链技术

侧链技术的主要动机是主流区块链效率低且功能有限, 如果将主链上的交易发生在性能更好的侧链上, 可以减少主链处理交易的压力. PeggedSidechains 是第 1 个使比特币等加密货币可以在不同区块链系统之间转移的侧链技术, 其提出的双向锚定协议是侧链技术最主要的特点. 双向锚定技术使得主链和侧链之间相对独立, 安全性不会相互影响, 实现交易的转移有助于提高扩展性. 侧链扩展方法如图 12 所示, 已有的侧链方案有根链 (root stock, RSK)[66]和 Plasma[67]等.

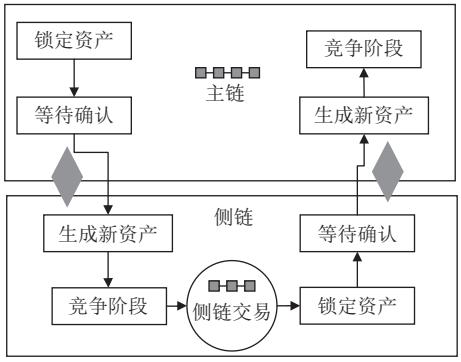

图 12 侧链技术原理

RSK 是第 1 个与比特币双向锚定的侧链. RSK 融合侧链和合并挖矿模型, 合并挖矿是一种同时在两条区块链上产生区块的技术. RSK 使得智能合约可以以比特币作为加密货币来执行, 开放性和使用 PoW 和合并挖矿使得 RSK 具备和比特币主链一样的安全性. RSK 使用 DECORE+协议来鼓励矿工从而避免矿工之间的冲突. RSK 可以实现更高的可扩展性并且降低交易成本, 提高交易吞吐量, RSK 可以使得比特币交易按照每秒 300–1 000 的速度被处理. RSK 也有一些缺点: (1) 它要求用户在进行交易之前先存入一些比特币; (2) 由于 RSK 是基于 PoW 的, 通过支持 SHA-256D 合并挖矿, 它的能耗很高.

Plasma 是一种融合侧链技术和分片思想的技术. 相比其他侧链方案给出更加完备的安全性证明. Plasma 的基本思想是在区块链中创建区块链如图 13 所示. 具体而言, Plasma 是一个基于 MapReduce 概念的框架, 用于构建可扩展的、非中心化的应用, 其中 MapReduce 是一个用于处理大数据集的框架. Plasma 结构是通过使用智能合约和默克尔树来构建的, 可以创建无数的子链. 在 Plasma 中可以创建更多的链形成一个树状结构, 每个 Plasma 子链都是一个用于不同的需求的定制化智能合约. 这些子链可以共存, 独立运行. 父链和子链之间的通信由防欺诈措施来保障; 父链负责保持网络的安全, 并负责惩罚恶意的参与者.

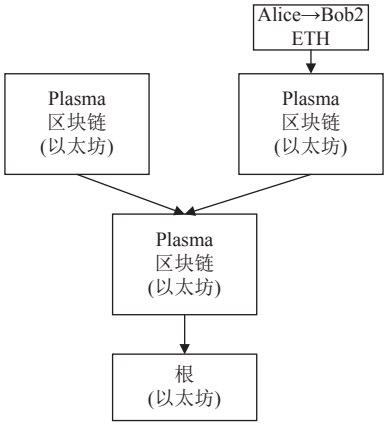

图 13 Plasma 结构

Plasma 受到广泛关注, 有很多研究者对其进行多种形式的实现. 但是, Plasma 框架仍然有许多限制, 包括: (1) 由于当时的以太坊智能合约中所有权的特征, 用完整的以太坊虚拟机功能可视化 Plasma 链是不合理的; (2) Plasma 中概述的确认签名也是有局限性的, 它们要求双方发送确认交易以确保最终性; (3) 对于希望提取资金的用户来说, 等待期很长 (7–14 天).

3.3.4 跨链技术

近几年, 旨在实现多条链的资产转化和状态交互的跨链技术发展迅速, 通过连接多条区块链实现了更好的交互性和可扩展性. 与侧链技术最大的区别是跨链技术中不同链之间是平等的, 无依附关系. 跨链技术中, 一条链的节点不存储同个网络中其余链的全部交易. 相反, 它利用智能合约从一个成员网络传递交易到另一个成员网络. 早期的开源侧链项目 BlockStream[68]被看作是跨链技术的雏形.

迄今为止, 跨链技术已经包含多种实现形式, 有公证人机制、侧链/中继机制、哈希锁定. 公证人机制是最简单也最直接的实现跨链资产转移的方法, 需要借助第三方公证人作为中介, 因此需要对第三方公证人有很高的安全信任假设. 侧链/中继技术中的侧链是一个独立于主链的区块链系统, 通过设计按需定制的协议、账本、共识机制、智能合约等, 使用户可以在侧链上使用主链的代币进行跨链交易. 哈希锁定思想最早应用于闪电网络, 借助哈希锁保障资产的转移和提取.

公证人机制是目前应用最广泛、技术实现最简单的一种跨链机制. 公证人机制根据公证第三方形式的不同, 可以分为单公证人机制、多公证人机制以及分布式公证人机制. 单公证人机制由单一指定的独立节点或者机构充当, 多公证人机制由多个独立节点或者机构充当, 分布式公证人机制通过多方计算和随机抽取公证节点的方式实现. 公证人机制的代表项目主要有 Interledger[69], 该协议的核心思想在于: “Interledger”提供的可信第三方, 会向发送者保证, 他们的资金只有在“可信第三方”收到证明, 且接收方已经收到支付时, 才将资金转给连接者; 可信第三方也同时也保证连接者, 一旦他们完成了协议的最后部分, 他们就会收到发送方的资金.

侧链是一个独立于主链的区块链系统, 通过设计按需定制的协议、账本、共识机制、 智能合约等, 使用户可以在侧链上使用主链的代币进行跨链交易. 这种跨链交易中侧链与主链沟通的过程被称为双向锚定, 具体而言就是, 在主链上锁定交易后, 等量等值的代币才能在侧链上被释放, 而当等量等值的代币在侧链上被锁定时, 主链上的原始币就可以被释放了. 中继是对公证人机制和侧链机制的有效融合和延伸, 中继链旨在构造一个第三方公有链, 通过第三方公有链来进行跨链信息传递. 侧链/中继机制的代表项目主要有 BTC Relay[70], 该方案通过以太坊智能合约对比特币交易进行验证, 具体方法是 BTC-Relay 利用 BTC 区块头在以太坊上创建一个小型简要版的比特币区块链来方便验证. Cosmos[71]和 Polkadot[72]也是有代表性的中继链方案.

Cosmos 是一个由多个独立区块链系统构成的网络如图 14 所示, 包含中心和空间两种角色. 空间指的是各个不同的区块链系统, 中心负责检测其余区块链运行状态. 初始只有一个中心 (Cosmos hub), 其他的块链系统在中心

上扩展, 进行连接交互. 中心使用 PoS 加密货币并且具有简单有效的治理能力. 扩展的区块链利用跨链通信协议 (inter-blockchain communication protocol, IBC) 进行交互. Cosmos 基于 Tendermint 共识, 通过应用区块链接口 (application blockchain interface, ABCI) 协议和已有的区块链系统进行兼容. 事实上, Cosmos 开发了通用区块链框架便于多种区块链在此基础上进行开发和交互, HyperLedger Fabric 就是基于其开发的, 以太坊等不是基于该框架开发的区块链需要借助锚定空间 (peg zone) 进行桥接.

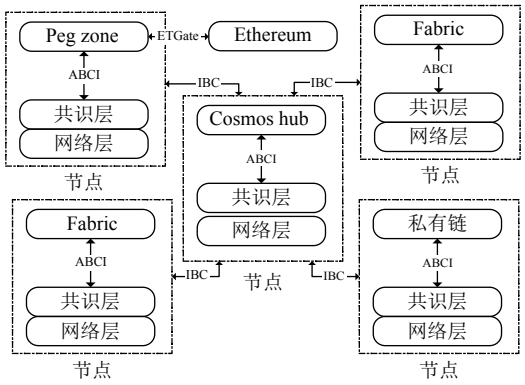

图 14 Cosmos 结构

Polkadot[72]是 2016 年提出的另一个跨链方案, 通过中继链的方式可以安全地在不同的独立区块链实现交互性和可扩展性. 中继链是一个非中心化的网络, 参与交互的区块链系统被称为 Parachains.

中继链为不同的 Parachains 提供了交互使用的安全接口. 中继链与内部的各个 Parachains 在结构和行为上相互独立, Polkadot 的中继链节点作为一个轻量级的节点运行 Polkadot 软件. 这些节点可以充当 3 种角色 (验证者、代理者、核对者), 在 3 个角色进行交互或者转换可以实现多个区块链系统的信息胡同, 提高整体网络的吞吐量.

哈希锁定, 全称哈希时间锁定合约. 哈希锁定技术原理是让交易双方先锁定链上的资产, 然后设置一个哈希锁 (哈希锁是指对一个哈希值 H, 如果提供原像 R 使得 $Hash(R) = H$, 则承诺有效, 否则失效), 如果都在规定的时间内输入正确哈希值的原值, 即可完成交易, 否则交易失效, 从而保证了交易的原子性. 然后再设置一个时间锁, 时间锁是指交易双方约定在某个有限的时间内输入正确哈希值的原值才有效, 超时则承诺失效.

跨链技术旨在实现多个链的交互, 没有像链内扩展一样提高区块链本身的吞吐量, 也不像其余链外扩展方案一样加快交易确认或者减轻某条区块链负担. 但是可以横向扩充区块链为一个网络, 增强多个区块链系统的链系, 提高区块链的可扩展性.

3.3.5 链下扩展技术总结

链下扩展技术主要通过扩展区块链的功能提高其可扩展性. 表 5 对链下扩展方案整体进行比较分析, 主要从吞吐量和延迟性能、是否加快交易确认、是否降低交易费用、安全性和非中心化因素考虑以及应用场景等方面, 对链下扩展各个技术的代表性方案进行分析对比.

对于吞吐量和延迟性能, 链下扩展更多地考虑对区块链应用层和合约层进行功能扩展, 往往涉及更多地区块链之外的交易处理、计算转义和多链交互等, 难以向链上扩展方案一样针对单一区块链给出直观的端到端性能指标. 对于状态通道和侧链技术, 吞吐量可用主链与通道 (侧链) 转移的交易总量来衡量, 相比于链上扩展技术, 链下扩展由于只需在主链上记录结果, 所以交易的成本低且速度快. 链下计算主要关注复杂计算的处理, 因此这类技术对于吞吐量往往取决于复杂交易本身的数量. 由于跨链技术强调多个区块链系统交互, 他们的吞吐量和延迟通常无法估量. 多数链下扩展方案在应用层进行交易处理, 具有很低的延迟.

除了延迟之外, 考虑链下扩展方案是否能够加快交易确认. 状态通道和侧链技术可实现链下交易和链上汇总的特点, 而且交易双方通常是提前可预知的, 可以快速确认交易. 链下计算和跨链通常不能加快区块链系统的交易确认.

表 5 链下扩展方案对比

方案	技术	吞吐量 (TPS)	延迟	加快交易确认	交易费用	实施难度	安全性	应用场景
闪电网络[58]#	状态通道	10^2	低	√	低	易	交易数据无隐私保护	支付
Trinity[60]		N/A	低	√	低	易		支付
TrueBit[63]*	链下计算	$<10^2$	低	×	N/A	易	交易数据无隐私保护	特殊
Arbitrum[64]*		$<10^2$	低	×	N/A	易		特殊
RSK[66]	侧链技术	3×10^2–10^3	低	√	低	中	主侧链安全性独立	任意
Plasma[67]		10^3	N/A	√	低	难	更强的安全性证明	任意
Cosmos[71]	跨链技术	10^3–2×10^4	N/A	×	N/A	难	中心链需安全假设	支付
Pokadot[72]		N/A	N/A	×	N/A	难		支付

注: #闪电网络由于使用人数较少, 实际值在10^2级别, 理论值可达10^6. *链下计算并不直接提高吞吐量, 等同于以太坊, 但是可以执行复杂的计算

考虑在实现功能扩展时各个方案的成本, 主要包含交易费用和实施难度两个指标. 交易费用指的是在实现交易转移或者合约执行时需要付出的额外费用. 其中链下计算方案不同的合约处理方式不一样, 跨链技术不同的区块链也会有不同的措施. 而状态通道和侧链技术一般不需要额外的开销, 状态通道仅需在通道建立和关闭时抵押资金, 侧链也会在资金转移结束后返回抵押金.

对于安全性和中心化问题, 相比于链上扩展技术, 链下扩展大多会更多地牺牲中心化程度, 引入中心化设施可能会引起用户的隐私问题等.

因为对区块链功能性扩展, 多数链下扩展方案无法适用于任意场景, 如状态通道和跨链通常用于支付场景, 链下计算则需要考虑特定的使用需求.

4 区块链可扩展性的总结与展望

本节给出对网络扩展, 链上扩展, 链下扩展各个方向技术的优缺点比较见表 6. 这些归纳通过宏观分析当前研究者的关注点, 有助于研究者思考区块链可扩展性领域的热点和难点, 以进行下一步研究. 在归纳可扩展性方案优缺点基础上, 本文进一步讨论区块链可扩展性的未来研究点, 希望可以激发研究者们解决区块链可扩展性问题的灵感, 主要包含以下展望.

(1) 混合可扩展性方案展望: 单一的方案难以在权衡安全性的同时有效解决区块链的可扩展性问题. 多数已有的工作提供有限的可扩展性提升或者引入新的安全问题. 然而, 两个或者更多的方案结合也许可以得到更好更安全的可扩展性方案, 本文认为是未来关注点混合方案是未来研究点之一, 如以太坊 2.0 采用分片和 Casper 协议混合.

(2) 提高区块链的数据读取性能展望: 读取性能会影响区块链可扩展性, 但是这个方向的研究甚少. 比特币的简单支付验证 (simplified payment verification, SPV) 节点和性能受限的 IoT 节点难以存储整个区块链, 依靠区块链服务器获取区块链数据. 然而区块链服务器的响应速度远低于本地的服务器, 因此很有必要提高区块链的读取性能. 其次, 与关系型数据库 MySQL 和非关系型数据库 NoSQL 相比, 区块链缺乏高效的查询语言和结构.

(3) 轻量存储且安全的新型链结构展望: DAG 结构使得区块链可以并发地追加区块到系统, 但是已有的 DAG 结构有大量的存储数据以及安全性和非中心化问题, 并且结构复杂, DAG 结构内区块之间的关系确认耗费时间和计算, 且当网络规模庞大时, 这些时间成本和计算成本成倍数增长, 高昂的时间成本和空间成本导致难以推广使用. 因此, 设计安全的、简洁高效的新型链结构且具备低存储并满足非中心化是未来研究点之一.

(4) 高效的分片划分和跨片交互方法展望: 分片是扩展区块链的有效方法, 但是低效的分片方法和跨片交互导致新的安全性和可扩展性问题. 越小越多的分片对于扩展性提升越大, 但是对于威胁的容忍性会降低, 本文认为解决这一问题是未来研究点.

表 6 扩展方案优缺点比较

分类	技术	相关文献	优点	缺点
网络扩展	中继网络和分发网络	bloXroute[18]	不影响区块链运行 可与上层扩展兼容	技术实现不太成熟 技术实现成本较大
	优化OSI模型	Nexus[19]	优化网络数据处理 可与上层扩展兼容	可扩展性提升有限
	改进信息传播	Erlay[22]	节约信息传播开销 具有一定的隐私性	可扩展性提升有限
链上扩展	优化区块数据	BitcoinCash[28] SegWit[29] Compact Block Relay[30]	区块包含更多交易 解决交易扩容问题	交易确认时间增多 链上分叉威胁增大
	分片	Elastico[31] OmniLedger[32] RapidChain[33] Monixide[34]	可以并行处理交易 只需处理片内交易 减少单节点的压力	整体的安全性较低 方案实现比较复杂
	共识协议	Bitcoin-NG[39] GHOST[40] FruitChains[42] Ouroboros[43] Dumbo[45] Byzcoin[51]	交易的确认延迟低 方案设计易于实现	整体的安全性较低
	新型链结构	Inclusive[53] Conflux[54] OHIE[56] Prism[57]	交易吞吐量有提高 节约节点计算能力	安全性的证明困难 难以做到强一致性 节点存储大量数据
链下扩展	状态通道	闪电网络[58] 雷电网络[59] Trinity[60] μRaiden[61]	支持及时支付场景 每笔交易费用降低	无法支持大额交易 要求资产抵押锁定
	链下计算	rollup[62] TrueBit[63] Arbitrum[64]	节点没有冗余计算 任务可以并行计算	可能存在隐私问题 可能引入安全威胁
	侧链技术	RootStock[66] Plasma[67]	可实现链的交互性 链安全性互不影响	主链频繁检查子链 主链存在存储负担
	跨链技术	BlockStream[68] Cosmos[71] Polkadot[72]	更好的链可扩展性 可实现链的交互性	依赖中心化的设计

References:

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

[2] Zeng SQ, Huo R, Huang T, Liu J, Wang S, Feng W. Survey of blockchain: Principle, progress and application. Journal on Communications, 2020, 41(1): 134–151 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000-436x.2020027]

[3] Li JJ, Yuan Y, Wang FY. Blockchain-based digital currency: The state of the art and future trends. Acta Automatica Sinica, 2021, 47(4): 715–729 (in Chinese with English abstract). [doi: 10.16383/j.aas.c210018]

[4] Yao Q, Zhang DW. Survey on identity management in blockchain. Ruan Jian Xue Bao/Journal of Software, 2021, 32(7): 2260–2286 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6309.htm [doi: 10.13328/j.cnki.jos.006309]

[5] Yuan Y, Zhou T, Zhou AY, Duan YC, Wang FY. Blockchain technology: From data intelligence to knowledge automation. Acta Automatica Sinica, 2017, 43(9): 1485–1490 (in Chinese with English abstract).

[6] Cai T, Lin H, Chen WH, Zheng ZB, Yu Y. Efficient blockchain-empowered data sharing incentive scheme for Internet of Things. Ruan Jian Xue Bao/Journal of Software, 2021, 32(4): 953–972 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6229.htm [doi: 10.13328/j.cnki.jos.006229]

[7] Cai XQ, Deng Y, Zhang L, Shi JC, Chen Q, Zheng WL, Liu ZQ, Long Y, Wang K, Li C, Guo MY. The principle and core technology of blockchain. Chinese Journal of Computers, 2021, 44(1): 84−131 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2021.00084]

[8] Xia Q, Dou WS, Guo KW, Liang G, Zuo C, Zhang FJ. Survey on blockchain consensus protocol. Ruan Jian Xue Bao/Journal of Software, 2021, 32(2): 277−299 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6150.htm [doi: 10.13328/j.cnki.jos.006150]

[9] Meng WT, Zhang DW. Optimization scheme for HyperLedger Fabric consensus mechanism. Acta Automatica Sinica, 2021, 47(8): 1885−1898 (in Chinese with English abstract). [doi: 10.16383/j.aas.c190516]

[10] Gaži P, Kiayias A, Zindros D. Proof-of-stake sidechains. In: Proc. of the 2019 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2019. 139−156. [doi: 10.1109/SP.2019.00040]

[11] Zhu JM, Zhang QN, Gao S, Ding QY, Yuan LP. Privacy preserving and trustworthy federated learning model based on blockchain. Chinese Journal of Computers, 2021, 44(12): 2464−2484 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2021.02464]

[12] Yuan Y, Ni XQ, Zeng S, Wang FY. Blockchain consensus algorithms: The state of the art and future trends. Acta Automatica Sinica, 2018, 44(11): 2011−2022 (in Chinese with English abstract). [doi: 10.16383/j.aas.2018.c180268]

[13] Bai C. State-of-the-art and future trends of blockchain based on dag structure. In: Proc. of the 8th Int'l Workshop on Structured Object-oriented Formal Language and Method. Gold Coast: Springer, 2019. 183−196. [doi: 10.1007/978-3-030-13651-2_11]

[14] Li Y, Men JB, Yu H, Wang SN, Fan JG, Guo YL. Overview of blockchain capacity expansion technology. Electric Power Information and Communication Technology, 2020, 18(6): 1−9 (in Chinese with English abstract). [doi: 10.16543/j.2095-641x.electric.power.ict.2020.06.00]

[15] Matt C. Compact block relay. 2016. https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki

[16] Matt C. FIBRE: Fast Internet bitcoin relay engine. 2019. https://github.com/bitcoinfibre/

[17] Soumya B. Decentralization in Bitcoin and Ethereum networks. arXiv:1801.03998, 2018.

[18] Klarman U, Basu S, Kuzmanovic A, Sirer EG. bloXroute: A scalabletrustless blockchain distribution network whitepaper. 2019. https://bloxroute.com/wp-content/uploads/2019/11/bloXrouteWhitepaper.pdf

[19] Karp H, Melbardis R. Nexus Mutual: A peer-to-peer discretionary mutualon the Ethereum blockchain. 2017. https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf

[20] Puneet K. QUIC (quick UDP Internet connections)—A quick study. arXiv:2010.03059, 2020.

[21] Team Harmony. Harmony technical white paper v2.0. 2018. https://harmony.one/whitepaper.pdf

[22] Naumenko G, Maxwell G, Wuille P, Fedorova A, Beschastnikh I. Erlay: Efficient transaction relay for bitcoin. In: Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security. London: ACM, 2019. 817−831. [doi: 10.1145/3319535.3354237]

[23] Chawla N, Behrens HW, Tapp D, Boscovic D, Candan KS. Velocity: Scalability improvements in block propagation through rateless erasure coding. In: Proc. of the 2019 IEEE Int'l Conf. on Blockchain and Cryptocurrency (ICBC). Seoul: IEEE, 2019. 447−454. [doi: 10.1109/BLOC.2019.8751427]

[24] Rohrer E, Tschorsch F. Kadcast: A structured approach to broadcast in blockchain networks. In: Proc. of the 1st ACM Conf. on Advances in Financial Technologies. Zurich: ACM, 2019. 199−213. [doi: 10.1145/3318041.3355469]

[25] Ozisik AP, Andresen G, Levine BN, Tapp D, Bissias G, Katkuri S. Graphene: Efficient interactive set reconciliation applied to blockchain propagation. In: Proc. of the 2019 ACM Special Interest Group on Data Communication. Beijing: ACM, 2019. 303−317. [doi: 10.1145/3341302.3342082]

[26] Xie JF, Yu FR, Huang T, Xie RC, Liu J, Liu YJ. A survey on the scalability of blockchain systems. IEEE Network, 2019, 33(5): 166−173. [doi: 10.1109/MNET.001.1800290]

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

[28] Kwon Y, Kim H, Shin J, Kim Y. Bitcoin vs. bitcoin cash: Coexistence or downfall of bitcoin cash? In: Proc. of the 2019 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2019. 935−951. [doi: 10.1109/SP.2019.00075]

[29] Kedziora M, Pieprzka D, Jozwiak I, Liu YX, Song HB. Analysis of segregated witness implementation for increasing efficiency and security of the bitcoin cryptocurrency. Journal of Information and Telecommunication, 2023, 7(1): 44−55. [doi: 10.1080/24751839.2022.2122301]

[30] Nagayama R, Shudo K, Banno R. Simulation of the bitcoin network considering compact block relay and Internet improvements. arXiv:1912.05208, 2020.

[31] Luu L, Narayanan V, Zheng CD, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proc. of the 2016

ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 17–30. [doi: 10.1145/2976749.2978389]

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

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

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

[35] Hellings J, Sadoghi M. ByShard: Sharding in a Byzantine environment. Proc. of the VLDB Endowment, 2021, 14(11): 2230–2243. [doi: 10.14778/3476249.3476275]

[36] Dang H, Dinh TTA, Loghin F, Chang EC, Lin Q, Ooi BC. Towards scaling blockchain systems via sharding. In: Proc. of the 2019 Int'l Conf. on Management of Data. Amsterdam: ACM, 2019. 123–140. [doi: 10.1145/3299869.3319889]

[37] Amiri MJ, Agrawal D, El Abbadi A. SharPer: Sharding permissioned blockchains over network clusters. In: Proc. of the 2021 Int'l Conf. on Management of Data. Virtual Event: ACM, 2021. 76–88. [doi: 10.1145/3448016.3452807]

[38] Zheng PL, Xu QQ, Zheng ZB, Zhou ZY, Yan Y, Zhang H. Meepo: Sharded consortium blockchain. In: Proc. of the 37th IEEE Int'l Conf. on Data Engineering (ICDE). Chania: IEEE, 2021. 1847–1852. [doi: 10.1109/ICDE51399.2021.00165]

[39] Eyal I, Gencer AE, Sirer EG, Van Renesse R. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the 13th USENIX Conf. on Networked Systems Design and Implementation. Santa Clara: USENIX Association, 2016. 45–59.

[40] Sompolinsky Y, Wyborski S, Zohar A. PHANTOM GHOSTDAG: A scalable generalization of Nakamoto consensus: September 2, 2021. In: Proc. of the 3rd ACM Conf. on Advances in Financial Technologies. Arlington: ACM, 2021. 57–70. [doi: 10.1145/3479722.3480990]

[41] Rizun PR. Subchains: A technique to scale bitcoin and improve the user experience. Ledger, 2016, 1: 38–52. [doi: 10.5195/ledger.2016.40]

[42] Pass R, Shi E. FruitChainss: A fair blockchain. In: Proc. of the 2017 ACM Symp. on Principles of Distributed Computing. Washington: ACM, 2017. 315–324. [doi: 10.1145/3087801.3087809]

[43] Kerber T, Kiayias A, Kohlweiss M, Zikas V. Ouroboros crypsinous: Privacy-preserving proof-of-stake. In: Proc. of the 2019 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2019. 157–174. [doi: 10.1109/SP.2019.00063]

[44] de Castro D, Polychroniadou A. Lightweight, maliciously secure verifiable function secret sharing. In: Proc. of the 41st Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Trondheim: Springer, 2022. 150–179. [doi: 10.1007/978-3-031-06944-4_6]

[45] Guo BY, Lu ZL, Tang Q, Xu J, Zhang ZF. Dumbo: Faster asynchronous BFT protocols. In: Proc. of the 2020 ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2020. 803–818. [doi: 10.1145/3372297.3417262]

[46] Yin MF, Malkhi D, Reiter MK, Gueta GG, Abraham I. HotStuff: BFT consensus with linearity and responsiveness. In: Proc. of the 2019 ACM Symp. on Principles of Distributed Computing. Toronto: ACM, 2020. 347–356. [doi: 10.1145/3293611.3331591]

[47] Peng ZS, Zhang YF, Xu Q, Liu HX, Gao YX, Li XH, Yu G. NeuChain: A fast permissioned blockchain system with deterministic ordering. Proc. of the VLDB Endowment, 2022, 15(11): 2585–2598. [doi: 10.14778/3551793.3551816]

[48] Amiri MJ, Agrawal D, El Abbadi A. CAPER: A cross-application permissioned blockchain. Proc. of the VLDB Endowment, 2019, 12(11): 1385–1398. [doi: 10.14778/3342263.3342275]

[49] Amiri MJ, Loo BT, Agrawal D, El Abbadi A. Qanaat: A scalable multi-enterprise permissioned blockchain system with confidentiality guarantees. Proc. of the VLDB Endowment, 2022, 15(11): 2839–2852. [doi: 10.14778/3551793.3551835]

[50] Nawab F, Sadoghi M. Blockplane: A global-scale Byzantizing middleware. In: Proc. of the 35th IEEE Int'l Conf. on Data Engineering. Macao: IEEE, 2019. 124–135. [doi: 10.1109/ICDE.2019.00020]

[51] Kokoris-Kogias E, Jovanovic P, Gailly N, Khoffi I, Gasser L, Ford B. Enhancing bitcoin security and performance with strong consistency via collective signing. In: Proc. of the 25th USENIX Conf. on Security Symp. Austin: USENIX Association, 2016. 279–296.

[52] Biais B, Bisière C, Bouvard M, Casamatta C. The blockchain folk theorem. The Review of Financial Studies, 2019, 32(5): 1662–1715. [doi: 10.1093/rfs/hhy095]

[53] Lewenberg Y, Sompolinsky Y, Zohar A. Inclusive block chain protocols. In: Proc. of the 19th Int'l Conf. on Financial Cryptography and Data Security. San Juan: Springer, 2015. 528–547. [doi: 10.1007/978-3-662-47854-7_33]

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

[55] Pawar V, Shelly S. ParallelChain: A scalable healthcare framework with low-energy consumption using blockchain. In: Proc. of the 2023 Int'l Trans. in Operational Research. 2023. 1–29.

[56] Yu HF, Nikolić I, Hou RM, Saxena P. OHIE: Blockchain scaling made simple. In: Proc. of the 2020 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2020. 90–105. [doi: 10.1109/SP40000.2020.00008]

[57] Bagaria V, Kannan S, Tse D, Fanti G, Viswanath P. Prism: Deconstructing the blockchain to approach physical limits. In: Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security. London: ACM, 2019. 585–602. [doi: 10.1145/3319535.3363213]

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

[59] Avarikioti G, Janssen G, Wang YY, Wattenhofer R. Payment network design with fees. In: Proc. of the 2018 ESORICS Int'l Workshops on Data Privacy Management, Cryptocurrencies and Blockchain Technology. Barcelona: Springer, 2018. 76–84. [doi: 10.1007/978-3-030-00305-0_6]

[60] TeamTrinity. Trinity: Universal off-chain scaling solution. 2019. https://trinity.tech/#/whitepaper

[61] Cirstea L. µRaiden: A payment channel framework for fast & free off-chain ERC20 token transfers. 2019. https://raiden.network/

[62] A rollup-centric ethereum roadmap. 2020. https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap

[63] Jason T, Christian R. A scalable verification solution for blockchains. arXiv:1908.04756, 2019.

[64] Kalodner H, Goldfeder S, Chen XQ, Weinberg SM, Felten EW. Arbitrum: Scalable, private smart contracts. In: Proc. of the 27th USENIX Conf. on Security Symp. Baltimore: USENIX Association, 2018. 1353–1370.

[65] Xu C, Zhang C, Xu JL, Pei J. SlimChain: Scaling blockchain transactions through off-chain storage and parallel processing. Proc. of the VLDB Endowment, 2021, 14(11): 2314–2326. [doi: 10.14778/3476249.3476283]

[66] Sergio D. RSK: A Bitcoin sidechain with stateful smart-contracts. IACR Cryptol. 2022. https://eprint.iacr.org/2022/684

[67] Poon J, Buterin V. Plasma: Scalable autonomous smart contracts. 2017. https://www.plasma.io/plasma-deprecated.pdf

[68] Siris VA, Dimopoulos D, Fotiou N, Voulgaris S, Polyzos GC. Interledger smart contracts for decentralized authorization to constrained things. In: Proc. of the 2019 IEEE INFOCOM—IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS). Paris: IEEE, 2019. 336–341. [doi: 10.1109/INFCOMW.2019.8845275]

[69] Hope-Bailie A, Thomas S. Interledger: Creating a standard for payments. In: Proc. of the 25th Int'l Conf. Companion on World Wide Web. Montréal: International World Wide Web Conf. Steering Committee, 2016. 281–282. [doi: 10.1145/2872518.2889307]

[70] ETHEREUM. Welcome to BTC relay's documentation. 2020. http://btcrelay.org

[71] Kwon J, Buchman E. Cosmos: A network of distributed ledgers. 2016. https://cosmos. network/whitepaper

[72] Wood G. POLKADOT: Vision for a heterogeneous multi-chain framework. 2016. https://polkadot. network/PolkaDotPaper.pdf

附中文参考文献:

[2] 曾诗钦, 霍如, 黄韬, 刘江, 汪硕, 冯伟. 区块链技术研究综述: 原理、进展与应用. 通信学报, 2020, 41(1): 134–151. [doi: 10.11959/j.issn.1000-436x.2020027]

[3] 李娟娟, 袁勇, 王飞跃. 基于区块链的数字货币发展现状与展望. 自动化学报, 2021, 47(4): 715–729. [doi: 10.16383/j.aas.c210018]

[4] 姚前, 张大伟. 区块链系统中身份管理技术研究综述. 软件学报, 2021, 32(7): 2260–2286. http://www.jos.org.cn/1000-9825/6309.htm [doi: 10.13328/j.cnki.jos.006309]

[5] 袁勇, 周涛, 周傲英, 段永朝, 王飞跃. 区块链技术: 从数据智能到知识自动化. 自动化学报, 2017, 43(9): 1485–1490.

[6] 蔡婷, 林晖, 陈武辉, 郑子彬, 余阳. 区块链赋能的高效物联网数据激励共享方案. 软件学报, 2021, 32(4): 953–972. http://www.jos.org.cn/1000-9825/6229.htm [doi: 10.13328/j.cnki.jos.006229]

[7] 蔡晓晴, 邓尧, 张亮, 史久琛, 陈全, 郑文立, 刘志强, 龙宇, 王堃, 李超, 过敏意. 区块链原理及其核心技术. 计算机学报, 2021, 44(1): 84–131. [doi: 10.11897/SP.J.1016.2021.00084]

[8] 夏清, 窦文生, 郭凯文, 梁赓, 左春, 张凤军. 区块链共识协议综述. 软件学报, 2021, 32(2): 277–299. http://www.jos.org.cn/1000-9825/6150.htm [doi: 10.13328/j.cnki.jos.006150]

[9] 孟吴同, 张大伟. HyperLedger Fabric共识机制优化方案. 自动化学报, 2021, 47(8): 1885–1898. [doi: 10.16383/j.aas.c190516]

[11] 朱建明, 张沁楠, 高胜, 丁庆洋, 袁丽萍. 基于区块链的隐私保护可信联邦学习模型. 计算机学报, 2021, 44(12): 2464–2484. [doi: 10.11897/SP.J.1016.2021.02464]

[12] 袁勇, 倪晓春, 曾帅, 王飞跃. 区块链共识算法的发展现状与展望. 自动化学报, 2018, 44(11): 2011–2022. [doi: 10.16383/j.aas.2018.c180268]

[14] 李洋, 门进宝, 余晗, 王思宁, 范金刚, 郭艳来. 区块链扩容技术研究综述. 电力信息与通信技术, 2020, 18(6): 1–9. [doi: 10.16543/j.2095-641x.electric.power.ict.2020.06.00]

陈晶(1981－), 男, 博士, 教授, 博士生导师, 主要研究领域为网络安全, 分布式系统安全, 区块链.

李凯(1997－), 男, 硕士, 主要研究领域为区块链, 应用密码学.

杨浩(1999－), 男, 硕士生, 主要研究领域为区块链, 应用密码学.

加梦(1996－), 女, 博士生, 主要研究领域为区块链, 应用密码学.

何琨(1986－), 男, 博士, 副教授, CCF 专业会员, 主要研究领域为应用密码学, 网络安全, 云计算安全, 人工智能安全, 区块链安全.

杜瑞颖(1964－), 女, 博士, 教授, 博士生导师, 主要研究领域为网络安全, 隐私保护.