网络首发时间：2023-02-27 10:57:07
网络首发地址：https://kns.cnki.net/kcms/detail//11.2127.TP.20230224.1812.014.html

区块链系统性能优化关键方法综述

宋传罡[1]， 李雷孝[1]， 高昊昱[2]

1.内蒙古工业大学 数据科学与应用学院，呼和浩特 010080
2.海南大学 网络空间安全学院（密码学院），海口 570228

摘 要：区块链是结合分布式架构、密码学以及激励机制等方法构建的一个分布式系统，具有不可篡改性、去中心化和不可伪造性等特点，实现了在不受信任的环境下实现安全的点对点交易，受到广泛关注。但是区块链技术存在着系统效能较低的问题，无法被大规模落地应用。从区块链的数据结构和发展趋势出发，对目前区块链存在的性能问题进行了分析，针对存在的问题，从链上扩容、链下扩容两个方面进行归纳讨论，从分片、有向无环图等主流方法全面总结分析了目前区块链扩容技术的最新研究进展并且在链上扩容部分加入了与深度强化学习相结合的优化方法，并在最后对未来的区块链优化方向提出了展望，以期对未来区块链吞吐量提升的研究提供参考和借鉴。

关键词：区块链；性能提升；深度强化学习；去中心化

文献标志码: A 中图分类号: TP309.2 doi：10.3778/j.issn.1002-8331.2211-0457

Review of key technologies for blockchain system performance optimization

SONG Chuangang[1], LI Leixiao[1], GAO Haoyu[2]
1. School of Data Science and Application, Inner Mongolia University of Technology, Hohhot 010080, China
2. School of Cyberspace Security (School of Cryptography), Hainan University, Haikou 570228

Abstract: Blockchain is a distributed system built by combining distributed architecture, cryptography and incentive mechanism, which has the characteristics of immutability, decentralization and unforgeability, and realizes secure peer-to-peer transactions in an untrusted environment, which has attracted widespread attention. However, blockchain technology has the problem of low system efficiency and cannot be applied on a large scale. Starting from the data structure and development trend of blockchain, the current performance problems are analyzed, and the existing problems are summarized and discussed from the two aspects of on-chain expansion and off-chain expansion, and the latest research progress of the current blockchain expansion scheme technology is comprehensively expounded from the mainstream aspects such as sharding and directed acyclic graphs, and the optimization method combined with the deep reinforcement learning method is added to the on-chain expansion part, and finally the future blockchain optimization direction is proposed. In order to provide reference and reference for the future research on blockchain throughput improvement.

Key words: blockchain; performance improvement; deep reinforcement learning; decentralization

区块链技术是目前被广泛关注的技术之一，已经在多个领域内投入应用，如开发了支持智能合约的公共区块链平台以太坊。目前区块链领域最新的主流发展方向是以应用为主题的区块链 3.0。区块链技术能够在不同领域发挥作用，如提高医疗数据的可信性并且提升数据安全[1]，供应链追踪[2]、社交[3]和存储安全[4]等应用。

基金项目：内蒙古自治区科技成果转化专项资金项目（2021CG0033），内蒙古自治区重点研发与成果转化计划项目（2022YFSJ0013），内蒙古自治区高等学校青年科技英才支持计划项目（NJYT22084）。

作者简介：宋传罡(1997－),男,硕士研究生, ,研究方向为区块链、网络空间安全;**李雷孝**(1978－),通信作者，男，博士，教授，CCF 专业会员，研究方向智能交通运输大数据、云计算与大数据分析,E-mail: llxhappy@126.com;高昊昱(1994－)，博士研究生，主要研究方向为区块链技术、共识算法、可信计算。

区块链技术具有去中心化、不可篡改的特点，能够解决网络中的信任问题和保证数据的安全性，但是区块链系统的性能问题限制着区块链的应用。经典的区块链应用如比特币与以太坊，都是优先了去中心化与安全性，降低了可扩展性的优先级。比特币的每秒处理事务数量(TransactionPerSecond，TPS)仅为 7 笔，而以太坊的 TPS 为 10-20 笔，与主流的中心化的支付交易系统差距过大。例如国内银行卡的银联系统，TPS 峰值可以达到每秒 24 万笔交易。低吞吐量引起区块链网络中的交易不断堆积，交易处理时间也变得越来越长，这导致了区块链技术在实时交易的领域无法有效运用。且伴随着分布式应用的增多，链上压力会增大，导致了区块链的吞吐量进一步降低，极大限制了区块链应用。

区块链系统中每个验证节点需要保存完整的账本历史数据和相应的状态信息，导致区块链系统会占用大量的存储资源。随着区块链规模不断扩大，账本的数据量也不断增加，因此区块链上用于存储信息的磁盘空间也会越来越大[5]。未来区块链上存储的账本信息甚至超过 1TB，目前大部分的商用计算机存储上限还未到达 1TB 的容量。数据量的增加，意味着从区块链中检索信息的速度会变慢，为了提高交易与验证的效率，验证节点会增加验证状态的索引[6]。在验证节点中引入索引会增加节点对于内存的需求。分级存储的方式可以有效缓减这一需求，超出容量的部分会保存在二级存储器中，但是二级存储器容易遭受分布式拒绝攻击。

针对上述区块链中存在的~~应用~~性能上的问题，本文以提升区块链系统性能为研究目标，并且将目前对于区块链的优化方法进行了概述。本文的组织结构如下：第一节对区块链技术进行了简要的介绍。第二节从链上扩容方式对区块链性能优化方法进行分类总结。第三节从链下扩容优化方法进行分类总结。第四节提出对目前有的区块链优化方法所存在的问题与对未来发展方向的展望。第五节总结了本文内容。

1 研究背景

1.1 区块链概述

区块链作为一种新兴技术，结合了分布式共识、密码学知识、时间戳以及激励机制等方法，实现了在无信任环境去中心化的点对点交易与协调协作[7]。区块链有着去中心化、高安全性以及透明性等特点，解决了传统的中心化模式可靠性不足、成本较高等固有问题[8]。区块链使用哈希函数生成哈希值，前一区块生成的哈希值会添加到后一区块，实现区块链的链式结构。当链式结构形成后，存放在区块链中的交易不可篡改。区块链技术可以使用匿名技术对真实世界的地址进行隐藏，保证了区块链的隐私性与匿名性。在区块链中任何节点都可以获取到保存在区块链中的交易信息，保证了区块链的透明性。另外区块链中使用了共识算法，通过合适的共识算法使每个节点之间直接形成共识，保证了数据的一致性。

根据去中心化程度的不同，区块链可以分为公有链、私有链、联盟链以及混合链：1）公有链无特定的所有者，在区块链网络中对所有节点都是开放的；2）私有链降低了区块链的去中心化特性，会选择一些特定的节点参与区块链共识，限制节点的参与资格，具有更快的交易速度和更低的交易成本；3）联盟链是许多机构共同参与建设，允许数据在系统内的不同结构进行之间读写与发送交易，并共同存储交易记录；4）混合链中所有节点拥有着不同的权限，部分节点权限为查看部分区块链数据，部分节点能够将区块链中全部的账本数据，部分节点仅负责记账。混合链具有其他类型区块链的特点，应用场景更广。

1.2 区块链共识机制

为了保证分布式集群中的全部节点能够拥有相同的数据并对存在问题形成一致意见，区块链中的共识机制[9]被提出。共识机制是区块链的核心部分，共识机制是否有效决定着区块链系统是否安全和区块链系统是否高效率运行。合理的共识机制能够使区块链协商形成整体的一致结构。主流的共识机制有工作量共识机制和权益证明机制。

工作量共识机制（Proof of Work，PoW）[10]被提出是为了在比特币网络中确定节点的记账权。利用节点自身的算力解决 SHA256 计算问题，通过寻找合适的随机数 Nonce 设定目标值，节点之间竞争计算能力来获得记账权，以确保数据一致性与安全性。权益证明（Proof of Work, PoS）[11]取消了 PoW 中的挖矿过程，使用权益证明的方式来决定记账权。持有币的人拥有记账权，投票权是根据持有币的多少来决定的，拥有币的数量越多所具备的话语权就越大。PoS 共识机制中的打包和投票是被分开的，使用的随机分配的方法选择打包区块的节点，其他的节点作为验证者，验证者会验证打包形成的新区块，拥有投票权的节点投票对区块进行验证之后，获得多数节点支持的区块被允许加入共识，形成一个有效区块。PoS 存在一个委员会系统，委员会投票决定区块的生成，并且委员会需要经常变换其中的成员。DPoS 是在 PoS 的基础提出的新的共识机制。DPoS 的基本框架是在 PoS 的基础上在持有股权的节点中选取出代表节点，代表节点负责运营区块链网络，每个授权代表节点在获得资格前需要缴纳一定的保证金。实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）[12]降低了 PoW 中需要的计算资源与电力资源，更适用于企业用联盟链。在 PBFT 中，恶意节点不超过全网节点数 1/3 即可保证异步分布式系统的安全性。

1.3 区块链优化方法

随着区块链规模的不断扩大，传统的区块链很难满足用户需求。为了应对传统区块链技术性能不足的挑战，众多专家学者对区块链的可拓展性和效果进行了分析。为了更加全面探讨区块链性能优化方法，通过分析总结相关文献对区块链优化方法进行分类，区块链系统性能优化方法主要划分为链上和链下两个角度，区块链优化方法研究框架如图 1 所示。

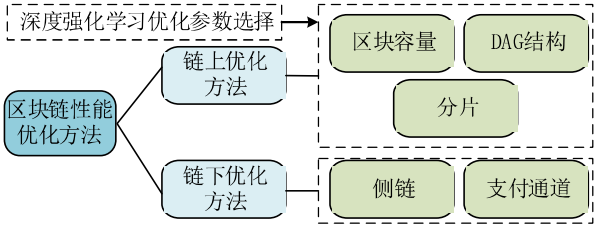

图 1 区块链优化方法研究框架

Fig.1 Blockchain optimization method research framework

2 链上扩容优化方法

链上扩容优化方法是指通过对区块链的规则进行修改来优化区块链系统性能，区块链链上扩容主要方法分为扩大区块的存储容量，有向无环图(Directed acyclic graph，DAG)、分片方案和利用深度强化学习动态优化。

2.1 增加区块容量

增加区块链中的区块容量是一种直接的提升区块链性能的方法，通过对区块容量进行改进，使得每个区块中存储更多的交易，提升区块链系统的性能。为了有效增大区块容量，在比特币系统中提出一系列与区块扩容相关的改进方案。比特币改进提案（Bitcoin Improvement Proposals，BIP）是在比特币社区中，用于表示在比特币中的新开发功能、流程与环境。比特币改进提案扩容协议的主要内容如表 1 所示。

目前比特币社区中主要的扩容协议分为两类方向，将区块的大小设置为固定值和浮动决定区块的大小。针对两种不同的区块扩容方向，比特币社区中一直存在争议而无法达成共识。由表 1 可得，直接增加区块容量是一种直观的区块链扩容方法，能够有效的提高区块能容纳的交易的数量，但是区块容量增大后不可避免的会导致网络传播效率降低、单独块出现的几率增大和增加分叉的可能，并不能真正解决底层问题。

表 1 区块链扩容协议

Table 1 Blockchain scaling protocols

协议编号	协议内容	提出者	协议局限性
BIP 100	移除 1MB 区块大小上限，将上限调整至 32MB，并且将区块大小浮动限制 1MB 到 32MB	Jeff Garzik	矿工可以自由决定区块大小，存在矿工无成本售出投票权的情况
BIP 101	获得全网 75%算力支持，将区块的大小限制到 8MB，然后将区块大小与时间线性联系，随时间增长区块大小增长，最大到达 8GB	Gavin Andresen	区块增长的速度过快
BIP 102	一次性扩容区块链，将区块大小设置为 2MB	Jeff Garzik	区块增大，区块链的中心化程度加大
BIP 103	提出将最晚生成的 11 个区块大小的中位数设置为区块大小的上限，从 2017 年至 2063 年，将区块大小限制提高 17.7%	Pieter Wuille	传播效率降低，空块率也会提升
BIP 105	将区块大小初始值设为 1MB，通过矿工投票决定提升或降低区块的大小，最大提升减少幅度设为 10%	Btc Drak	矿工权力增大，更容易出现作恶的情况
BIP 106	根据难度调整区块大小上限，每 2000 个区块为一个调整周期，以 90%的区块为基准，如果这些区块大小到达上限的 90%，区块的大小上限将会扩大两倍，如果大小小于上限的 50%，区块链大小上限将会减半	Upal Chakraborty	区块个体大小增大，容易导致区块链网络的传输延迟增大
BIP 107	按阶段进行扩容，在 2016 至 2017 为 2MB，2018 至 2019 为 4MB，2020 年到达 8MB，此后按每四周为一个周期，决定是否提升上限大小	Washington Y Sanches	区块个体大小增大，容易导致区块链网络的传输延迟增大
BIP 109	对区块限制提升到 2M 大小	Gavin Andresen	产生硬分叉，与原有区块链网络不兼容

2.2 有向无环图

有向无环图(Directed Acyclic Graph，DAG)是一种为了优化单链结构的低效率而应用的一种新的区块链数据结构。传统的区块链数据结构是一条单链结构，除创世节点不含前驱区块，其他任意区块存在前驱区块并且仅有一个前驱区块。区块的出块时间决定了区块在区块链中的前后顺序，通过哈希指针链接前后区块。这种串行数据结构导致区块链之间的性能受到限制。为了解决单链结构不足，DAG 中任意的基本单元既可以与多个前驱单元链接，也可以与多个后驱单元链接。DAG 结构与传统区块链数据结构相比，能够有效提升区块链系统性能，由于 DAG 结构中不要求矿工验证每一个交易，只需要验证父交易即可，这种方式能够减少矿工工作量，出块时间相应的也可以压缩。

2.2.1 DAG 区块链系统结构

IOTA（Internet of Things Application）是面向物联网行业设计的无限权分布式账本，联合了机器设备和正在发展的新技术实现费用更低的交易并且保证数据完整性，给未来物联网发展提供方向[13]。IOTA 的建立基础是分布式账本技术 Tangle，Tangle 中用 DAG 结构取代了传统连续链式结构。Tangle 使用 Winternitz 的签名方式，Winternitz 签名是基于散列的签名，可以提升交易处理速度，并能够帮助系统同时处理多个交易。在 Tangle 网络没有设定区块奖励机制，进行交易需要验证过往交易部分，这使得交易费为 0，因此在 Tangle 网络中实现微交易是可能的。Tangle 协议一个关键功能是通过网络协议，并且允许节点交换验证过的身份与加密过的数据。IOTA Tangle 的出现促进了区块链系统开始应用 DAG 数据结构。

DAG 区块链系统的结构如图 2 所示，将有向无环图结构应用到区块链中，区块通过存储不同父区块的哈希值来与不同的父区块链接。DAG 架构减少了区块链网络中挖矿者的数量，降低了真实交易的费用，区块链交易费用降低后使得 DAG 具有处理微型交易的能力。最早将 DAG 结构运用到区块链加密货币的是 NXT，NTX 在 2013 年作为新一代加密货币，采用了 DAG 数据结构来代替传统链式结构并使用了基于 curve 25519 算法生成密钥，使其每秒处理的交易量可以提升至千次并保证了区块链系统的安全性。使用 DAG 区块链结构矿工的挖矿时间没有变化，但是可储存的交易扩展了数倍，网络中同时存在的区块数量也能够提升[14]。

由于 DAG 结构具有更加快速的处理速度，DAG 应用到区块链系统的研究受到广大学者关注。Byteball[15]是一个应用了 DAG 结构的去中心化系统，通过设置见证节点和主链的方法来实现去中心化，建立交易的初始会形成由数个只负责发布交易的见证节点组成的群体。见证节点的作用是在交易列表中选择一笔交易回溯到创世交易，然后加入创世交易的主链中。新交易的不断发布主链数量也会增加，不同的主链会形成交叉，这个交叉点被称为稳定点。稳定点在主链移动，与稳定点链接的交易也会被确认，然后形成确定序列。在 Byteball 中每个交易都会获得发起交易的发起者的私钥签名，新生成交易都会与已经结束的交易联系，便于对新交易的验证，这使得安全性得到了保证。

由于 Byteball 是使用关系数据库来存放数据，这会使得 Byteball 拓展性与速度收到影响。NANO[16]是目前应用了 DAG 的分布式账本技术，它的数据结构被设计为栅格结构（block-lattice）。采用栅格结构 NANO 中的每一个账户会拥有一个单独的链条，这种方式可以降低区块链的瞬时交易时间。通过栅格结构，并发系统效率获得提升，不同的账户之间独立进行交易，加快了交易处理的速度。

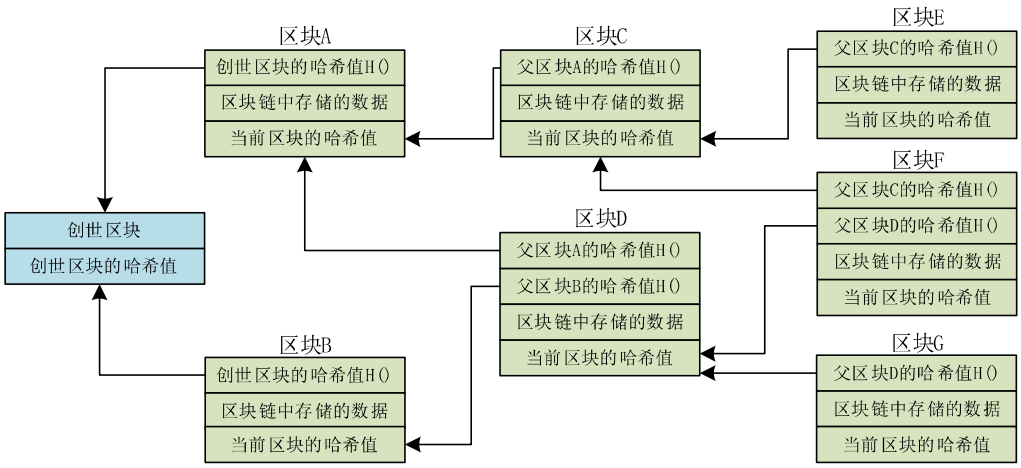

图 2　区块链有向无环图结构

Fig.2　Structured acyclic graph of blockchain

2.2.2 DAG 区块链优化

目前针对 DAG 的研究在迅速发展，许多学者对基于 DAG 的方法提出优化改进。DAG 区块链具有可扩展性、不可兼容性等特点，对 DAG 区块链在不同方面进行优化，以适应各种不同场景。现在对于 DAG 区块链的优化主要总结为三个方面，对交易速度的优化、整体结构的优化和安全性优化。

1）交易速度的优化：DAG 区块链网络交易确认速度优化能够增进 DAG 区块链网络性能，Wang 等人[17]构建了一个基于 DAG 的系统 3D-DAG，3D-DAG 网络中由提供交易与资产转移的基础主链、基于状态的侧链和主链与侧链的链接通信三个方面组成，这种设计方法可以改善传统区块链系统主链的负载过大的弊端，提升分布式应用性能。为了解决耗能问题和协议在特定环境下没法有效运行的问题，Zhou 等人[18]提出了一个双 DAG 体系无限权区块链 DLattice，它使用了 Double-DAG 架构，在结构中每个账户有专属 account-DAG，全部节点组成 Node-DAG 架构，在此结构中账户之间互不影响，并且在账户 D-Tree 中使用红黑默克尔树加速查询和增加数据的效率。Wang 等人[19]为了优化区块链交易对 Tangle 结构进行改进，提出了一种新的 Re-Tangle 结构。这种结构将 Tangle 的运行过程转化成为 ReRAM 矩阵向量乘法运算，将 Re-Tangle 分为 Random Walking Module 与 Validation Module。对于共识算法方面，Ferraro 等人[20]开发了 IOTA DAG 的流体模型，并且在延迟偏微分模型的基础上，提出了 hybrid tip selection algorithm，解决了 DAG 区块链出现的分叉问题。此外，除了 DAG 的共识算法方面，Saad 等人[21]叙述了 DAG 渐变过程，提出了一种辅助数据通信协议 MAM，能够增强通过 DAG 释放与访问数据流能力。

2）存储结构优化：DAG 区块链存储结构方面的优化也可以给区块链系统效率带来提升，Gupta 等人[22]使用了图形的数据结构代替了区块链中传统的链式结构 GraphChain[23]，并提出应用收敛有效无环图 CDAG 结构替代 DAG 结构来更好的提升区块链效率。Xiang 等人[24]提出了一种基于 DAG 的共识算法 Jointgraph，在此共识中，打包到事务中的交易需要由 2/3 的成员验证，并且在共识中设定了监督人的存在，有效提升了共识的效率。

3）安全性优化：DAG 区块链安全方面的优化能够保证区块链中的交易顺利进行，Pervez 等人[25]对不同的 DAG 区块链进行了比较分析，并且设计了安全的 DAG 区块链框架。Cui 等人[26]基于 DAG 提出了一种新的安全的区块链协议 CoDAG，CoDAG 中的区块按照级别进行组成，并且通过小幅度的修改现有 DAG 结构来保持原有简单架构。Nguyen 等人[27]提出了新的共识协议 STAIR，实现在不可信环境下的 DAG 系统高效的完成协商。

综上所述，利用 DAG 技术可以有效的提升区块链性能问题，基于 DAG 结构的区块链也受到广大学者关注，并对 DAG 区块链的优化开展深入研究。DAG 区块链在各种领域开展应用，如在智能电网网络中，利用基于 DAG 的分布式账本 PowerGraph[28]在智能电网生成验证网络中的交易，并且能够跟踪能源交易以及各种类型的交易，实现对数据的完全追踪。虽然 DAG 区块链拥有交易速度快和吞吐量高等优点，但是在单笔交易的安全问题上存在隐患。

2.3 分片

区块链分片技术是通过将整体区块链网络进行分片，从而实现提升区块链系统的性能。分片技术在区块链技术出现之前已经在数据库系统中广泛应用，主要作用是对数据库的优化。分片技术的作用原理是将数据库中数据进行分割，把数量庞大的数据变为合理的数据分片，然后将这些数据分片分别分配到不同的服务器中来进行存储[29]。

为了增强区块链的可扩展性，分片被广泛认为是一种有前途的解决方案。分片后区块链网络形成数个子网络，每个子网络中存储着区块链网络中的一部分节点。各个分片可以并行处理事务，可以在整个系统中并行创建和验证多个区块，提高了事务吞吐量。同时，分片允许大量区块链节点参与，因为委员会规模更小从而没有增加通信、计算和存储开销[30]。分片技术的组成如图 3 所示，区块链网络中的节点进行分组，形成不同的初步共识组，不同的初步共识组会分到不同的交易。初步共识组对交易处理后会将结果发送到最终共识组，最终共识组生成最终区块增加到区块链主链上。

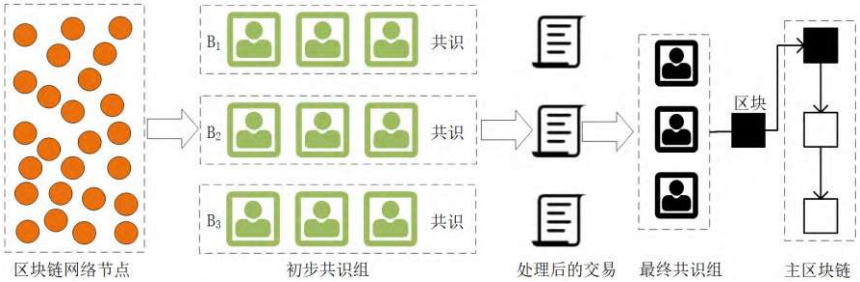

图 3 区块链分片技术

Fig.3 Blockchain sharding technology

2.3.1 区块链分片方法

区块链分片技术由以太坊中提出，根据面向的对象不同，分片方式可以分为网络分片、交易分片和状态分片[31]。网络分片是最易行的一种分片方案，也是交易分片与状态分片的基础。网络分片会将整体的区块链网络分为子网络，分片的过程需要保证随机性和合理性，每个子网络形成一个分片，分片能够并行处理区块链网络中的不同交易。交易分片是指将区块链网络中完成的交易分配到不同的分片中，然后每个分片中进行共识，每个分片验证交易数据是使用并行处理的方式进行的，从而有效的提高全网性能。状态分片构成较为复杂，每个节点负责存储特定的部分账本数据，不再存储全部账本信息，内部账本信息由每个分片自身负责维护，减少了系统处理事务的压力。

1）网络分片应用：在区块链分片中，首先要实现网络分片，一般使用随机函数来进行分片的流程。Elastico 使用 epochRandomness 函数来计算 Nonce，根据 Nonce 值确定分片位置，随后进行广播，RapidChain[32]只进行一次 Bootstrap 环节来确定分片配置，后续连续的共识过程与重配置过程，分片配置环节中会在低层节点持续构造 sampler graph。然后将每个 group 中哈希值最小节点汇总组成 subgroup，subgroup 继续进行随机组合，直到选出负责选择参考委员会（Reference Committee）成员的 root group。

2）交易分片应用：在片内各节点的交流可以直接通过广播的方式，但在跨片进行共识的时候需要以各个分片为单位进行交流，主要方式为交易原子化与交易集中化。交易原子化是将原交易进行分解，降低交易大小，生成子交易。如 OmniLedger[33]提出了 Atomix 协议，客户端发起跨片交易，不同的分片对子交易验证，当交易通过验证后，客户端会发送接收凭证的资金解锁请求到将要输出交易的分片，完成交易。交易集中化是对跨片交易统一发送到指点的链上或者指定节点上进行处理。在 Ethereum 2.0 中提出了，信标链（Beacon Chain）负责连接主链和对分片的管理。信标链是使用的 Casper FFG 共识，可以监管 Ethereum 2.0 中的跨分片交易是否收到双花攻击，并最终确定各个分片。

3）状态分片应用：为降低数据冗余，对跨分片交易进行优化，对状态分片又可以分为全分片存储和半分片存储[34]，OmniLedger 是全分片存储账本，每个分片存储不同的数据，跨片共识协议完成验证数据过程，节点配置过程中需要与分片间数据进行交接。为了解决账户状态不合理问题，BrokerChain[35]使用了一种新的动态划分调整分片状态的新架构，根据历史交易信息构建账户状态图并根据图对分片的账户状态动态调整与重配置。半分片存储时不同分片共同创建维持账本信息，Hong 等[36]提出了一种新的区块链系统 Pyramid，该系统实现了层级分片，制定了桥接分片来存储其他分片的区块，而且桥接分片可以直接对跨片交易进行验证，并且实现共识，从而有效提升系统吞吐量。为了满足大规模物联网设备对区块链性能的需求，Zheng[37]等人提出了 Aeolus 状态分片方法，通过额外参数根据不同分片将智能合约执行划分为不同状态，同一分片的不同状态按照顺序进行执行。

2.3.2 区块链分片共识协议

分片配置后区块链系统会进行共识操作，主要分为片内共识与跨片共识，片内共识中每一个分片可以进行共识算法的选择，如 PoW 共识算法、PoS 共识算法和 BFT 改进算法等，通过广播的方式能够进行直接交互。分片与分片之间也需要一种共识算法，用于将独立的分片连接成一个整体。分片共识协议的选择显著的影响着区块链系统的性能。

传统的区块链共识算法应用在分片后的区块链节点中也是适用的。PoW 共识算法是一种通过计算消耗算力取得记账权的算法，基于 PoW 的片内共识协议在计算中会生成身份编号，可以作为打包区块的标志符。SSChain[38]和 Monoxide[39]分片内使用的共识协议为 PoW，Monoxide 在一个 PoW 问题时间内出少于剩余分片数量的区块，然后由生成的区块交由其他的分片验证，验证通过后再次出块。每个分片共识组防御能力为 51%，出块时会对多个将要出块的块头利用 Hash 函数联合计算，这些将要出块的块头使用的 Nonce 是相同的，编号为 b 的共识组将生成的 m 个块头排序组成 Merkle 树。<MerkleRoot，b，m，Nonce> 会作为参数参与 Hash 计算，出块的同时，相应的消息会被广播到特定的共识组，确定在每个分片中只有一个区块生成，不会被延迟的出块影响。

有些区块链分片系统会使用 BFT 算法进行共识，Elastico 中使用的 PBFT，OmniLedger 中使用的是改进的 ByzCoinX，RapidChain 使用的是 gossip，BFT 共识协议通过分片内的各个节点验证共识。Zilliqa 使用两轮 ECSChnorr 多重签名[40]代替传统 PBFT 共识中 prepare 和 commit 两个阶段，降低了算法的复杂性，提升效率。

跨分片共识协议是以分片为单位进行信息交流，在不同的分片间使用共识协议以达成跨片共识。分片达成共识的主要方式有交易拆分方法、交易集中方法和路由协议方法。

交易拆分方法是将原交易分解为最小的子交易，如 OmniLedger 中在进行跨片交易时会让不同的分片验证不同的子交易，验证通过后进行资金解锁从而完成此笔交易。交易拆分方法可以实现分片间的交流，但是容易出现资金锁定时间过长的问题和容易遭受 DDOS 攻击。

交易集中方法是分片间指定新的交易地址，将所有跨

片交易统一处理。在以太坊中就设计了一个信标链作为管理分片之间交互的核心。集中式的分片交易方法降低了跨分片交易的难度，但是牺牲了一定的去中心化。

路由协议方法是在 RipidChain 中提出的，利用路由的思想将分片视为一个个网络节点，通过路由传播的方法进行交易。

综上所述，分片方法有效的进行了优化区块链系统的吞吐量、时间延迟和鲁棒性。但是分片后的节点的数量降低，如何保证区块链的可信度问题和协议的安全性是未来需要重点关注的研究方向之一。

2.4 深度强化学习方法优化区块链性能

在设计区块链系统的过程中，开发人员需要耗费大量时间去调整参数，并且需要选择激励机制，共识算法，考虑安全性和其他很多方面细节的考虑。深度强化学习可以帮助去解决难题，实现区块链系统性能的提高。

人工智能是另一个备受关注的领域，传感器、社交媒体软件等应用产生大量的数据，能够帮助人工智能领域的快速发展[41]。深度强化学习（Deep reinforcement learning，DRL）是属于人工智能的子领域，主要由智能体（Agent）、环境（Environment）、状态（State）、动作（Action）、奖励（Reward）组成。深度强化学习核心思想是通过智能体与环境交互返回包含状态和环境的奖励，找到连续状态下的最优策略。深度强化学习可以在与环境的交互过程中通过调整策略来获得最大化期望回报，区块链与深度强化学习的结合被提出来为解决区块链系统的吞吐量问题，提供了新思路。区块链系统消耗大量计算能力来解决工作证明的无意义难题，另一方面，许多人工智能应用需要大量计算能力才能实现高性能。将深度强化学习方法与区块链结合可以平衡双方的不足和实现区块链性能的提升。

区块链可以为深度强化学习提供各种需要的组件，如深度强化学习所需要的数据集、算法与去中心化市场交易过程中的计算能力。区块链结合深度强化学习将系统效率与创新水平显著提高，如 Mamoshina 等人[42]在医疗系统中采用了去中心化的区块链模型，模型可以让用户直接将数据上传到医疗系统中，并将定价透明化。透明的定价将由数据价值模型确定，这样可以保证公平的追踪数据的使用动向。Woods[43]融合了人工智能技术与区块链技术，目的解决互联网快速发展中所面临的安全问题。目前 52%的流量由机器产生，随着网络的发展，机器与机器交互和人机交互明显增加，可以预见机器与机器交互将超越人机交互，在网络中大量交互的过程中，将会产生大量的流量。随着深度强化学习方法不断的提高与发展，结合深度强化学习的区块链系统可以实现与区块链环境交互并且自动选择最优行为。

2.4.1 深度强化学习方法

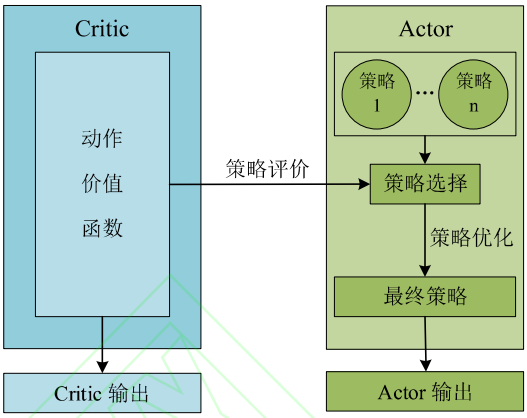

图 4 Actor-Critic 框架的 DDPG 流程

Fig.4 DDPG flow of the Actor-Critic framework

深度强化学习是把深度学习与强化学习相结合的一种人工智能方法。最早将卷积神经网络与传统强化学习相结合的是 Mnih[44]等人，深度 Q 网络是一种基于值函数的深度强化学习方法，因为传统的 Q 学习方法只能解决离散型的问题，如果问题是连续型的，传统 Q 学习方法是无法解决的，神经网络可以处理连续型的问题，将两者结合起来可以很好的处理传统 Q 学习无法处的连续问题。

策略梯度也是智能体学习的重要方式[45]，使用一些参数来控制我们的策略，给模型输入一个状态，然后模型输出相应的动作。深度策略梯度方法基本方法是利用不同的策略梯度去对神经网络中参数化策略进行优化，这种方法需要在每次迭代的时候获取一定数量的轨迹来更新策略梯度。但是训练数据的获取是非常困难的，将传统的 Actor-Critic Algorithm 加入到深度策略梯度方法中可以解决连续动作的特征会使收集的轨迹数据无法达到所需要的覆盖面的问题。

深度强化学习算法的优化收到国内外学者的广泛关注，Lillicrap 等人[46]对确定性策略梯度进行改造，提出了一种基于 Actor-Critic 框架的深度确定性策略梯度（DDPG），框架如图 4 所示，DDPG 能够处理连续动作空间上深度强化学习问题，使用两个参数分别去表示深度神经网络中的值函数与确定性策略。DDPG 中存在策略网络与值网络，设定两个网络的作用是对策略进行评价更新，值网络作用是逼近状态动作对的值函数，并且交付梯度信息。Heess 等人[47]设计了一种随机值梯度（SVG）的方法，利用再参数化[48]的方法来学习环境并且生成模型。对于经验回放机制的不足，Mnih 等人[49]结合异步强化学习的方法，提出了使用异步梯度下降法来改善网络控制的参数，目前异步 Actor-Critic Algorithm 是控制任务中表现最好的算法之一。

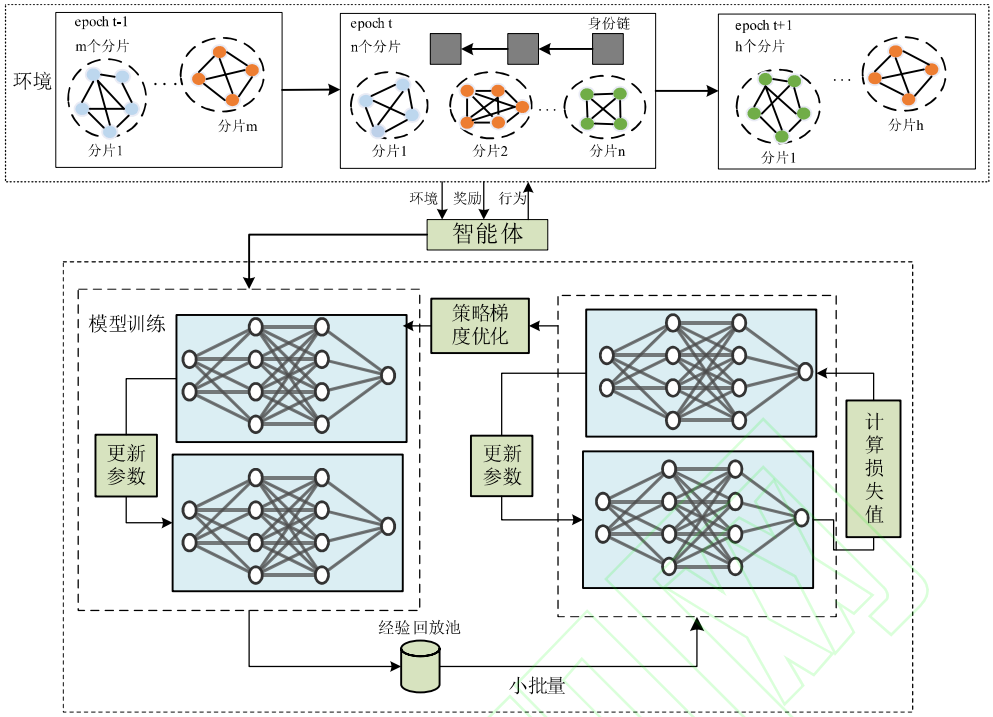

图 5 深度强化学习优化区块链分片技术

Fig.5 Deep reinforcement learning optimizes blockchain sharding technology

2.4.2 DRL 优化区块链分片

在区块链系统中可以使用分片方法来提升系统性能，分片技术分为静态优化方法和动态优化方法，使用静态优化方法即当在对区块链网络进行分片时，分片的策略一直是相同的[50,51]。动态优化方法即在进行区块链分片时，根据不同的情况选择不同的分片策略，动态优化方法更适合变化的区块链环境，因此可以将分片技术与深度强化学习进行结合，能够在变化的区块链环境中寻找最优的分片策略。

天空链[52]由 Jianting Zhang 等人将深度强化学习与区块链技术结合提出。为了解决区块链的可扩展问题，提出了一种基于动态分片的方法来应用到区块链系统，系统组成如图 5 所示。skychain 利用深度强化学习动态设计分片方法，通过神经网络动态调整分片的间隔、分片数量和区块大小来优化高维度系统状态上的区块链分片策略。深度强化学习智能体根据环境状态产生区块链分片行为，执行新的分片行为后的区块链系统会产生新的环境状态。当每个 epoch 结束时，事务池和下一个 epoch 的节点状态将成为 DRL 的新的环境输入。智能体与区块链系统的产生的数据会存储到经验回放池中，通过不断的训练寻找最优的分片方案。skychain 模型 epoch t 的关键部分（状态空间S_t，行为空间A_t，奖励R_t）定义如下

$$S_t=[q,m]_t \tag{1}$$

其中m表示区块链分片中的节点数，q表示尚未处理的交易。

$$A_t=[T_{epoch},k,S^B]_t \tag{2}$$

T_{epoch}表示 epoch 的长度，k表示分片数量，S^B表示区块大小。

$$R_t(S_t,A_t)=\begin{cases}\dfrac{k}{T_{epoch}}\dfrac{S^B}{S^T}R_C\dfrac{1}{R_r+1} & 满足\varphi_1—\varphi_3,\\ 0 & 不满足.\end{cases} \tag{3}$$

S^T表示交易的平均大小，R_r表示分片中平均冗余交易数，R_c表示公式过程中的轮数，φ是约束条件。

基于分片的可扩展区块链系统[53]是由 Jsusik Yun 等人提出，通过基于深度 Q 网络的分片区块链(deep Q network shard-based blockchain，DQNSB)来获取动态环境中的最佳配置方案。通过分析方程估计恶意程度，根据网络状态调整区块链参数，在保证了系统安全性的前提下自适应的优化系统的吞吐量。在 DQNSB 提出后，Wen[54]等人提出了基于分片的分支决斗网络区块链模型(branching dueling Q-network shard-based blockchain，BQNSB)，使用强化学习中的 branching dueling Q-network 算法来对区块链的分片过程进行优化，将分片的效率进一步提高。

YANG 等人[55]提出了一个能够支持分片区块链的物联网负载平衡优化框架。在物联网领域结合深度强化学习对区块链节点分片，对内部分片达成共识和最终形成的共

识进行理论分析，形成马尔可夫决策过程。在 DRL 智能体中联合训练事务池分配、区块间隔与区块大小，该框架可以有效提高物联网分片区块链系统的可扩展性。

深度强化学习方法不需要建立系统去分析模型，使用系统分片产生的历史数据就可以得到最优的分片策略，从而提高了区块链系统的性能。但是在区块链分片中使用的深度强化学习算法中行为空间随着行为维数的增加对应增加，导致深度强化学习算法效率降低，神经网络难以顺利训练。

2.4.3 DRL 结合区块链技术应用场景

区块链系统的低吞吐量导致其在各个领域中的应用收到很大限制，传统的方法一般从两个方面来处理：1）通过减少区块中事务的数量来提高吞吐量，但是这种方法会影响到区块在全网的广播效率[56]。2）处理事务时使用不同出块节点可以缩短区块生成时间，但是容易造成区块链分叉[57]。DRL 智能体可以对区块链环境进行学习，利用深度强化学习选择最优区块链参数可以有效优化传统提高吞吐量方法，目前不同领域的深度强化学习与区块链结合也在快速发展，区块链结合深度强化学习应用场景总结如表 2 所示。

在车联网领域，深度强化学习与区块链系统结合能够提升车联网中区块链系统的吞吐量。Lin 等人[64]将深度强化学习和区块链整合到 SDN-IOV 应用的空间众包过程中，提出了结合深度强化学习与区块链的空间众包系统。在此系统中，为了保护任务分配和发布中的任务隐私，使用了多区块链结构和结合区块链的分层分类任务管理模型，用基于深度强化学习的方法来进行任务分配。通过在安全的通信网络上以事务的形式存储众包任务，构建基于 Hyperledger 结构的私有区块链[65,66]。区块链克服了传统众包的单点故障问题，SDN-IOV 可以根据不同要求将任务划分不同的类别，并且根据不同安全级别的任务来构建子区块链，使用所提出的基于 DRL 的管理策略来动态选择共识算法、区块大小和区块生成规则，从而提高空间众包效率和安全性。

表 2　区块链结合深度强化学习应用总结

Table 2　Summary of applications of blockchain combined with deep reinforcement learning

应用领域	年份	文献	贡献
区块链结构	2020	[58]	提出针对区块链网络的深度强化学习自适应方法来提高区块链可拓展性
工业物联网	2021	[59]	将区块链系统问题表述为马尔可夫决策过程，使用基于深度 Q 学习的方法优化设备能效和系统计算开销
工业物联网	2019	[60]	利用 DRL 算法处理工业物联网区块链系统特征，动态选择区块生产者、共识算法、区块大小等
车联网	2019	[61]	提出基于 DRL 的 IoV 区块链性能优化框架，提高了系统的事务吞吐量
软件定义的工业互联网	2020	[62]	使用深度递归 Q 网络和归一化优势函数相结合解决马尔可夫决策过程问题，对区块链系统的性能进行优化
工业物联网	2020	[63]	将区块链缓存问题表述为马尔可夫决策过程，最小化智能合约的运行延迟

在电网配电中，使用深度强化学习和区块链技术可以有效提高配电效率与安全性。Qiu 等人[67]将深度强化学习、区块链和边缘卸载技术结合在微电网配电网络中，提出了一种协同边缘终端的任务处理框架，用来提高区块链系统的计算能力。建立了一种考虑区块链延迟与吞吐量的任务卸载模型，利用深度强化学习中的异步优势 Actor-Critic Algorithm 进行分配功率、设置区块大小与设置区块间隔，有效的提升了配电过程中的效率。

综上所述，将区块链技术与深度强化学习合理结合，将区块链系统中分片过程形成马尔科夫决策决策过程，在保证了安全性的前提提升了区块链的吞吐量，优化了区块链结构，在链上实现了区块链的拓展性。区块链技术与深度强化学习技术结合已经初步展现效果，开始被越来越多的学者将其应用到不同领域，但是作为一个新兴的领域，在隐私保护方面、智能合约安全、可扩展性、管理等方面有许多的研究问题需要解决。为了更加完善区块链与深度强化学习的结合和更好的发展两者，未来可以把现在的 DRL 框架拓展到每个区块链节点，使每个节点更加智能，从而更有效地保证数据共享的安全性。长时间的进行任务时，智能体会消耗大量时间并陷入死循环，开发高效的学习机制，从增加记忆组件，合作学习与分解任务等方面提高深度强化学习模型的记忆性与推理能力，使智能体的学习具有记忆力与可拓展性是深度强化学习结合区块链发展的主流方向。

3　链下扩容优化方法

链上扩容优化的方法对网络设备等要求较高，性能优化方面存在着许多限制。针对链上扩容优化方法的局限，众多学者开始对链下扩容优化方法进行研究。链下扩容优化方法不对区块链的规则进行直接改动，通过将数据交易执行和数据处理转移到链下进行处理，区块链只验证交易是否有效。链下扩容优化方法减轻了区块链上事务处理的压力，主要的链下扩容优化方案有侧链方法与支付通道方法。

3.1 侧链

侧链是为了增加区块链的可扩展性给主链提供支持服务的辅助区块链，在区块链系统中允许将新功能附加在侧链上。通过侧链可以用于小额支付的场景，由于小额支付不需要很高的安全等级，将交易过程从主区块链转移到侧链上，侧链可以使用不同的共识机制与选择任意数量的区块验证者以提高事务处理速度。侧链的运行机制如图 6 所示。

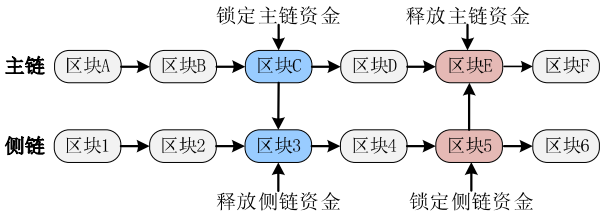

图 6 侧链运行机制

Fig.6 Operation mechanism of sidechain

3.1.1 侧链双向锚定模式

侧链技术是通过 Two-way Peg 的技术，利用主侧链管理用户的数字资产。当用户的数字资产在主链上固定，同时相同的数字资产会在侧链上释放，反之如果固定数字资产在侧链之上，主链上的相同数字资产会被释放。目前存在一些具体的方式，如单一托管模式、联盟模式、简单支付验证(Simplified Payment Verification，SPV)模式、驱动链模式和混合模式。

1）单一托管模式是由单一的托管方管理用户的数字资产，托管方通过确认信息激活侧链上的数字资产。单一托管模式可以保留当前的区块链协议，但是由于是单一托管方进行交易的管理，不可避免的提高了中心化的程度。

2）联盟模式使用公证人联盟方式，由多个节点组成一个公证人联盟，利用公证人多重签名模式对侧链上用户的数字资产变化进行确认。联盟模式同样的可以保留原始区块链协议，使用了公证人模式提高了数字资产的安全性，但是如果公证人存在恶意节点侧链的安全性不能得到保障。

3）SPV 模式中，数字资产会固定在主链上特定地址，当交易完成后，侧链会创建一个有 SPV 证明的交易，SPV 证明用来验证交易已经完成。在验证主链上的数字资产固定后，侧链会释放相同价值的数字资产，在使交易记录返回主链，对主链的数字资产进行更改。SPV 模式提高了侧链技术的安全性、隐私性和交易速度，但是主链会产生软分叉。

4）驱动链是利用矿工作为托管方对侧链的状态进行确认，提高了系统安全性，但是同样的会产生软分叉。

5）混合模式是对上述方法的有效结合，提升了系统的处理效率，但是也会产生软分叉。

双向锚定模式系统运行的前提要求参与者是可信的，如果存在不诚实的参与者，主链和侧链的资金可以同时被解锁，容易出现双花攻击。

3.1.2 侧链平台

区块链主链和侧链之间安全有效的交互成为目前侧链技术发展的主要方向，BTC Relay[68]是利用智能合约将以太坊网络与比特币网络进行连接，实现在以太坊平台上查看比特币网络中的相关信息。Plasma[69]设计了一个树状结构，在树状结构中将形成子链，主链将复杂繁重的计算任务转移到子链上进行，缓解主链的计算负担。Rollup[70]利用智能合约管理主链与子链之间的数据交互，对交易的状态进行打包与简单加密后，发送可用性证明代替所有的交易。

目前比较知名的侧链平台有 Loom，Proof-of-Authority (POA) Network，Liquid 和 RootStock (RSK)[71]。Loom Network 是一个能够与以太坊侧链链接，并且能够在侧链上运行 DApps 与游戏的平台。Loom Network 使用 DPoS 协议达成节点间的共识，可以快速的达成交易确认并提高吞吐量。POA 网络是开发智能合约的以太坊侧链，使用授权证明的共识方法来达成节点间的共识。POA 网络支持本地智能合约，允许智能合约和 DApp 从以太坊环境转移到 POA 网络。Liquid 是 Blockstreem 的商业侧链，可以无需等待区块链中的确认延时，完成瞬时交易。RSK 是链接比特币主网的开源侧链。RSK 降低了消费者在比特币平台上的交易时间，在 RSK 平台上每秒可以处理 300-1000 笔交易。 每个侧链平台的特点如表 3 所示。

侧链是为了缓解主链的计算压力过大问题而提出的新技术，由于侧链发展的时间较短，侧链平台多数还处于开发状态，在侧链平台中注册和提交 DApp 是很困难的，并且一些平台并未集成到比特币和以太坊的测试网络中，这使得侧链平台的发展受到限制，如何将侧链平台集成到主链中将是未来需要重点研究的方向之一。

表 3 侧链平台特点

Table 3 Features of sidechain platforms

平台	应用案例	共识协议	优势	局限性
Loom Network	Delegatecallh 游戏开发 DApp	Delegated Proof-of-Stake （DPoS）	游戏具有可拓 展性和高效率	仅限于 windows 系统支持 Token 存在安全风险 中心化问题
POA Network	智能合约拓展	Proof of Authority (PoA)	区块链之间的 交互	中心化问题 用户地域过于集中 共识机制存在安全隐患
Liquid	国际汇兑	proof of possession(POP)	交易速度更快	开放群体局限 资源消耗较大 中心化问题
RSK	零售支付系统 供应链跟踪 数字标识	PoW	执行智能合约 能力增强	开放群体局限 中心化问题

3.2 支付通道

3.2.1 支付通道运行原理

支付通道是在区块链系统中建立一条用户对用户或者是用户对服务的通道，然后将难以计算的问题转移到链外计算。只需要将计算结果返回到区块链上存储，计算结果需要由多方进行签名，保证了支付通道的安全性，支付通道的具体流程如图 7 所示。首先建立支付通道，交易双方将部分资金放入支付通道，然后在支付通道里进行交易，交易结束后会关闭支付通道，并将交易后的资金返回链上。根据交易方式的不同，将支付通道可以分为单向支付通道与双向支付通道。

单向通道的弊端过于明显，现在的支付通道主要以双向支付通道为主，主流支付通道应用有闪电网络[72]，雷电网络[73]等。闪电网络是在比特币社区中提出，为了解决区块链吞吐量低的问题的一个支付系统，能够支持小额交易并能有效提高区块链交易吞吐量。闪电网络通过序列到期可撤销合约（Recoverable Sequence Maturity Contract，RSMC）和哈希时间锁（Hashed Time Lock Contract，HTLC）来保证链下可信交易。RSMC 假定形成了支付通道，交易双方会预存资金到支付通道，然后在支付通道中进行交易。每次交易后更新资产分配方案并由双方确认，新更新的方案会直接取代旧方案。在交易双方需要提现时，会将交易方案写入区块链，然后进行确认。在确认时如果发现是使用的旧方案将会收取罚金给质疑者。HTLC 是通过智能合约来规定转账方通过多重签名地址对一部分钱进行冻结，通过哈希锁与时间锁，对资金的支出和支出时间做出了限制，保证了用户之间交易的安全。目前闪电网络已经开发了多路径支付的方法，将大额交易拆分成为小额交易，拆分后处理交易。雷电网络类似与闪电网络，是应用在以太坊上的提高事务吞吐量的方法，利用链下状态网络对以太坊处理能力进行拓展，用户能够私下的进行转账签名消息的转账，减轻了以太坊主网上的压力。

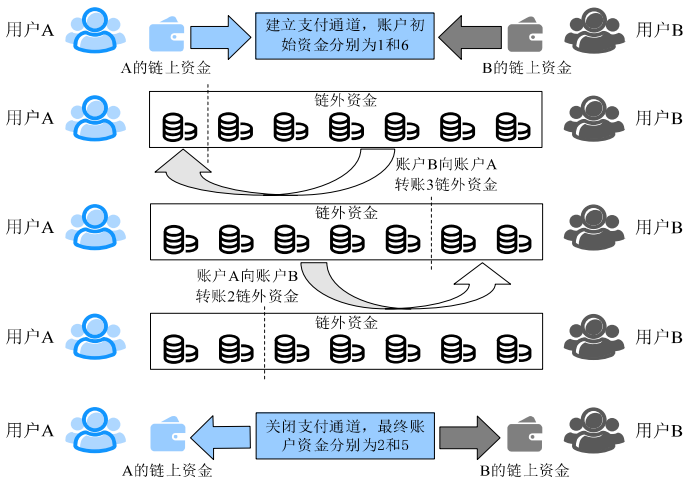

图 7 支付通道交易过程

Fig.7 Payment channel transaction process

双向支付通道方案在建立通道的同时也需要建立一个中间节点，中间节点的出现会影响区块链的去中心化。为了降低双向支付通道对区块链的去中心化特性的影响，Perun[74]设计了一种虚拟支付通道，直接将交易的双方使用虚拟通道连接起来，取消了中间节点。支付通道方案由于需要锁定一段时间的资金，容易被恶意节点攻击导致多个支付通道连接成的路径上资金全部锁定，形成悲伤攻击。在支付通道交易过程中，容易发生恶意节点攻击导致的资金锁定时间过长，EGGER 等[75]提出了一种新的计量方式，以避免资金锁定时间过长的情况发生和遭受悲伤攻击。

目前的支付通道的研究主要集中建立两方之间的支付通道，当出现多个节点参与的链下支付，一般使用支付划分的方法在多个支付通道内完成。使用划分交易的方法将增大交易的复杂度，增加了链上开销，Gnocchi[76]多人支付通道方法允许多个用户在一个信道内进行交易，并且设立监管节点来对提升链下通道状态的更新频率。但是 Gnocchi 不能应用在高并发的场景下，支付只能在通道内部进行。针对 Gnocchi 方案的局限性，Ge 等人[77]提出了支持高并发的多人链下支付方案，在 Gnocchi 方案之上进行改进，提出了支付有效期的方法来降低网络时延，将状态更新方式由串行更新转换成了并行更新。

3.2.2 支付通道路由算法对比分析

链下通道中的节点通过支付通道相互连通形成了支付通道网络，不同的节点可以直接实现资金转移或者通过中间节点进行资金转移。链下支付通道路由算法与传统路由算法存在差别，支付通道网络中需要考虑交易的状态，并且每个通道间具有方向性和限制金额，无法直接使用传统的路由方法进行路径的选择。目前，路由算法分为单路路由算法与多路路由算法，单路路由算法对交易不进行拆分，由一条路径实现资金的转移，在交易规模小的情况下应用较多。多路路由使用多条路径实现资金转移，对通道中的交易进行拆分，使用不同的通道进行交易，减轻了路径处理交易的压力，适用于交易规模较大的场景下。代表路由算法分类及其优缺点如表 4 所示。路由算法的选择与优化是区块链支付通道方法的关键，算法通过获取网络拓扑、通道容量和通道使用情况等信息，在支付通道网络中进行路径搜索，以获得最优路径。

支付通道网络路由算法提升了链下网络寻址的效率，但是寻路方案中并没有很好的保证通信双方隐私保护的问题，如 Flare 中付款方需要获得支付通道中的信息，不诚实节点可以装作付款方获取通道内的账户余额信息，侵犯了用户隐私。多数路由算法只关注于提高支付通道网络的寻址效率，网络路径中的通道信息很容易被恶意节点获取，未来需要重视支付通道中的隐私问题。

表 4　代表路由算法总结

Table　4 represents a summary of routing algorithms

文献	算法名称	算法原理	所属类别	优点	缺点
[78]	蚂蚁路由算法	网络节点通过保存周围的路由信息和与周边节点的通道状态，在三个阶段后找到交易双方节点的可行路径	单路路由	实现了去中心化的路由，不存在中心化特殊权限节点	通道中交易的安全性不足
[79]	Flare	节点只负责维护自己周围的相关视野，以路由表的形式存在，通过随机搜索的方法寻找合适的网络路径	单路路由	消耗的带宽较低	寻找路径的过程中存在失败的可能
[80]	SpeedyMurmurs	发送方将交易总额进行拆分，使用生成树的方法来寻找网络路径，并且设置固定坐标表示生成树中的节点	多路路由	提升了通道利用率	存在通道失衡的可能，增加网络中的开销
[81]	CoinExpress	引入容量锁机制，使用深度优先算法或者是广度优先算法获得可连通的网络路径，接受节点最终确定使用路径	多路路由	吞吐量显著提升，通信成本降低	地址需要公开，隐私安全性存在不足
[82]	cRoute	通过确定网络中的实时拥堵程度来确定路由方向	多路路由	更高的通道利用率和吞吐量	算法可拓展性存在不足
[83]	Spider network	当通道容量不足时，使用队列存储交易，等到通道恢复后队列中的交易继续进行	多路路由	保证通道的负载均衡，吞吐量显著提升	算法可拓展性存在不足

4　区块链性能优化技术展望

链上扩容优化方法和链下扩容优化方法能够一定程度上提升区块链系统的吞吐量，但是优化方法也有着局限性和不足，在文章的每一节对技术方面的不足做出了总结。链上扩容优化方法容易受限于网络中的节点数量，并且结构的直接优化同样存在着安全性问题，链下扩容方法面临着安全性不足、对计算结果的验证困难和调用智能合约困难等问题，在上述提出方法的基础上，下面给出未来研究方向。

4.1 链上扩容与链下扩容相结合

链上扩容方法主要在区块链自身结构进行优化，但是容易受到区块链网络的节点数和交易数的制约，优化性能有限。当区块增大时，验证区块的工作会增加，并且加大了区块的中心化，链下扩容通过将链上计算转移到链下，能够加快交易的速度，未来在链上扩容方法的基础上增加链下扩容的相关协议来提升交易的安全性和可扩展性。

4.2 增强链下扩容方法的隐私保护

由于链下通道需要将交易从区块链上转移到其他链上或者支付通道中，会造成余额信息、交易付款方和交易收款方等交易信息，未来增强链下交易的隐私性将成为重要的研究方向，例如使用英特尔软件保护拓展(Intel Software Guard Extension,SGX)来防止用户支付隐私的泄露。

4.3 结合深度强化学习优化区块链挖矿过程

深度强化学习与区块链的结合目前尚处于起步阶段，如何有效的发挥两者的特性是未来将要重点关注的工作，未来可以利用深度强化学习技术可以将区块链挖矿过程建模为马尔科夫决策过程，通过多智能体深度强化学习方法帮助矿工寻找最优的挖矿策略，提高区块链性能。

5 结束语

系统处理事务能力低下一直是制约区块链大规模应用的一大问题，导致区块链无法在日常生活中高吞吐量的场景中使用，并且会导致链上存储压力过大。许多研究人员针对区块链性能方面存在问题提出了许多解决方案。本文总结了解决区块链性能方面的方法，通过链上扩容、链下扩容两方面进行分析，总结了区块链优化技术的方法与分析存在问题，并对提高区块链性能技术未来发展方向提出了思考与总结。

参考文献

[1] MCBEE M P, WILCOX C. Blockchain technology: principles and applications in medical imaging[J]. Journal of digital imaging, 2020, 33: 726-734.

[2] 朱兴雄,何清素,郭善琪.区块链技术在供应链金融中的应用[J].中国流通经济,2018,32(03):111-119.
ZHU X X,HE Q S,GUO S Q. On the Role of Blockchai n Technology in Supply Chain Finance[J].China Circulatio n E-conomy,2018,32(03):111-119.

[3] LI C, PALANISAMY B. Incentivized blockchain-based social media platforms: A case study of steemit[C]//Pro- ceedings of the 10th ACM conference on web science. 2019: 145-154.

[4] CHEN Y, LI H, LI K, et al. An improved P2P file system scheme based on IPFS and Blockchain[C]//2017 IEEE International Conference on Big Data (Big Data). IEEE, 2017: 2652-2657.

[5] 曹雪莲,张建辉,刘波.区块链安全、隐私与性能问题研究综述[J].计算机集成制造系统,2021,27(07):2078-2094.
CAO X L,ZHANG J H,LIU B. Review on security, privacy, and performance issues of blockchain[J].Computer Inte grated Manufacturing Systems,2021,27(07):2078-2094

[6] 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[J].通信学报,2020,41(01):134-151.
ZENG S Q,HUO R,HUANG T,LIU J,WANG S,FENG W. Survey of blockchain: principle, progress and application [J].Journal on Communications,2020,41(01):134-151.

[7] WANG X, ZHA X, NI W, et al. Survey on blockchain for Internet of Things[J]. Computer Communications, 2019, 136: 10-29.

[8] XIA Q I, SIFAH E B, ASAMOAH K O, et al. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE access, 2017, 5: 14757- 14767.

[9] YUAN Y, NI X, ZENG S, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022.

[10] LEPORE C, CERIA M, VISCONTI A, et al. A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS[J]. Mathematics, 2020, 8(10): 1782.

[11] KING S, NADAL S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper, August, 2012, 19(1).

[12] ZHENG X, FENG W. Research on practical byzantine fault tolerant consensus algorithm based on blockchain[C]//Journal of Physics: Conference Series. IOP Publishing, 2021, 1802(3): 032022.

[13] GANGWANI P, PEREZ-PONS A, BHARDWAJ T, et al. Securing environmental IoT data using masked authentication messaging protocol in a DAG-based blockchain: IOTA tangle[J]. Future Internet, 2021, 13(12): 312.

[14] WANG S, LI H, CHEN J, et al. DAG blockchain-based lightweight authentication and authorization scheme for IoT devices[J]. Journal of Information Security and Applications, 2022, 66: 103134.

[15] DONG Z, ZHENG E, CHOON Y, et al. Dagbench: A performance evaluation framework for dag distributed ledgers[C]//2019 IEEE 12th international conference on cloud computing (CLOUD). IEEE, 2019: 264-271.

[16] LEMAHIEU C. Nano: A feeless distributed cryptocurrency network[EB/OJ].[2018-03-24].https://nano.org/en/whitepaper.

[17] WANG Q. Improving the scalability of blockchain through dag[C]//Proceedings of the 20th International Middleware Conference Doctoral Symposium. 2019: 34-35.

[18] ZHOU T, Li X, Zhao H. DLattice: A permission-less blockchain based on DPoS-BA-DAG consensus for data tokenization[J]. IEEE Access, 2019, 7: 39273-39287.

[19] WANG Q, WANG T, SHEN Z, et al. Re-tangle: A reram- based processing-in-memory architecture for transaction- based blockchain[C]//2019 IEEE/ACM International Con- ference on Computer-Aided Design (ICCAD). IEEE, 2019: 1-8.

[20] FERRARO P, KING C, SHORTEN R. On the stability of unverified transactions in a DAG-based distributed ledger[J]. IEEE Transactions on Automatic Control, 2019, 65(9): 3772-3783.

[21] SAAD A, PARK S Y. Decentralized directed acyclic graph based dlt network[C]//Proceedings of the International Con- ference on Omni-Layer Intelligent Systems. 2019: 158-163.

[22] KAN J, CHEN S, HUANG X. Improve blockchain performance using graph data structure and parallel mining[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018: 173-178.

[23] GUPTA H, JANAKIRAM D. CDAG: a serialized blockdag for permissioned blockchain[J]. arXiv preprint arXiv:1910. 08547, 2019.

[24] XIANG F, HUAIMIN W, PEICHANG S, et al. Jointgraph: A DAG-based efficient consensus algorithm for consortium blockchains[J]. Software: Practice and Experience, 2021, 51(10): 1987-1999.

[25] PERVEZ H, MUNEEB M, IRFAN M U, et al. A compar ative analysis of DAG-based blockchain architectures[C]// 2018 12th International conference on open source system s and technologies (ICOSST). IEEE, 2018: 27-34.

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

[27] NGUYEN Q, CRONJE A, KONG M, et al. Stairdag: Cr- oss-dag validation for scalable bft consensus[J]. arXiv pre- print arXiv:1908.11810, 2019.

[28] GAO Y, LIU Y, WEN Q, et al. Secure drone network edge service architecture guaranteed by DAG-based blockchain for flying automation under 5G[J]. Sensors, 2020, 20(21): 6209.

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

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

[31] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016: 17-30.

[32] ZAMANI M, MOVAHEDI M, RAYKOVA M. Rapidchain: Scaling blockchain via full sharding[C]//Proceedings of the 2018 ACM SIGSAC conference on computer and communi- cations security. 2018: 931-948.

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

[34] 黄华威,孔伟,彭肖文,郑子彬.区块链分片技术综述[J].计算机工程,2022,48(06):1-10.
HUANG H W,KONG W,PENG X W,ZHENG Z B. Surve- y on Blockchain Sharding Technology[J].Computer Enginee ring,2022,48(06):1-10.

[35] HUANG H, PENG X, ZHAN J, et al. BrokerChain: A Cross-Shard Blockchain Protocol for Account/Balance-based State Sharding[C]//IEEE INFOCOM. 2022.

[36] HONG Z, GUO S, LI P, et al. Pyramid: A layered shard- ing blockchain system[C]//IEEE INFOCOM 2021-IEEE C- onference on Computer Communications. IEEE, 2021: 1-1 0.

[37] ZHENG P, XU Q, LUO X, et al. Aeolus: Distributed Execution of Permissioned Blockchain Transactions via State Sharding[J]. IEEE Transactions on Industrial Informatics, 2022.

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

[39] WANG J, WANG H. Monoxide: Scale out blockchains with asynchronous consensus zones[C]//16th USENIX symposium on networked systems design and implementation (NSDI 19). 2019: 95-112.

[40] LIU Y, LIU J, LI D, et al. Fleetchain: A secure scalable and responsive blockchain achieving optimal sharding[C]// In ternational Conference on Algorithms and Architectures for Parallel Processing. Springer, Cham, 2020: 409-425.

[41] KOCH M. Artificial intelligence is becoming natural[J]. Cell, 2018, 173(3): 533.

[42] MAMOSHINA P, OJOMOKO L, YANOVICH Y, et al. C onverging blockchain and next-generation artificial intellige

nce technologies to decentralize and accelerate biomedical research and healthcare[J]. Oncotarget, 2018, 9(5): 5665.

[43] WOODS J. Blockchain: Rebalancing & Amplifying the Power of AI and Machine Learning (ML)[EB/OL]. [2018-08-03].https://medium.com/cryptooracle/blockchain-rebalancing-amplifying-the-power-of-ai-andmachine-learning-ml-af95616e9ad9.

[44] MNIH V, KAVUKCUOGLU K, SILVER D, et al. Playing atari with deep reinforcement learning[J]. arXiv preprint arXiv:1312.5602, 2013.

[45] LE N, RATHOUR V S, YAMAZAKI K, et al. Deep reinforcement learning in computer vision: a comprehensive survey[J]. Artificial Intelligence Review, 2022: 1-87.

[46] LILLICRAP T P, HUNT J J, PRITZEL A, et al. Continuous control with deep reinforcement learning[J]. arXiv preprint arXiv:1509.02971, 2015.

[47] HEESS N, WAYNE G, SILVER D, et al. Learning continuous control policies by stochastic value gradients[J]. Advances in neural information processing systems, 2015, 28.

[48] REZENDE D J, MOHAMED S, WIERSTRA D. Stochastic backpropagation and approximate inference in deep generative models[C]//International conference on machine learning. PMLR, 2014: 1278-1286.

[49] MNIH V, BADIA A P, MIRZA M, et al. Asynchronous methods for deep reinforcement learning[C]//International conference on machine learning. PMLR, 2016: 1928-1937.

[50] ZHANG M, LI J, CHEN Z, et al. An efficient and robust committee structure for sharding blockchain[J]. IEEE Transactions on Cloud Computing, 2022.

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

[52] ZHANG J, HONG Z, QIU X, et al. Skychain: A deep reinforcement learning-empowered dynamic blockchain sharding system[C]//49th International Conference on Parallel Processing-ICPP. 2020: 1-11.

[53] YUN J, GOH Y, CHUNG J M. DQN-based optimization framework for secure sharded blockchain systems[J]. IEEE Internet of Things Journal, 2020, 8(2): 708-722.

[54] 温建伟,姚冰冰,万剑雄,李雷孝.结合深度强化学习的区块链分片系统性能优化[J].计算机工程与应用, 2022, 58(19): 116-123.
WEN J Y, YAO B B, WAN J X, LI L X. Performance optimization of blockchain sharding system combined with deep reinforcement learning[J].Computer Engineering and Applications,2022,58(19):116-123.

[55] ZHAOXIN Y, RUIZHE Y, MENG L I, et al. A load balance optimization framework for sharded-blockchain enabled Internet of Things[J]. HIGH TECHNOLOGY LETTERS, 2022, 28(1): 10-20.

[56] DECKER C, WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels [C]//Symposium on Self-Stabilizing Systems. Springer, Cham, 2015: 3-18.

[57] KOGIAS E K, JOVANOVIC P, GAILLY N, et al. Enhancing bitcoin security and performance with strong consistency via collective signing[C]//25th usenix security symposium (usenix security 16). 2016: 279-296.

[58] QIU C, REN X, CAO Y, et al. Deep reinforcement learning empowered adaptivity for future blockchain networks[J]. IEEE Open Journal of the Computer Society, 2020, 2: 99-105.

[59] YANG L, LI M, SI P, et al. Energy-efficient resource allocation for blockchain-enabled industrial Internet of Things with deep reinforcement learning[J]. IEEE Internet of Things Journal, 2020, 8(4): 2318-2329.

[60] LIU M, YU F R, TENG Y, et al. Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3559-3570.

[61] LIU M, TENG Y, YU F R, et al. Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle[C]//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-6.

[62] LUO J, CHEN Q, YU F R, et al. Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning[J]. IEEE Internet of Things Journal, 2020, 7(6): 5466-5480.

[63] LIU P, YAO C, LI C, et al. A Caching-Enabled Permissioned Blockchain Framework for Industrial Internet of Things based on Deep Reinforcement Learning[J]. 2022.

[64] LIN H, GARG S, HU J, et al. Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(6): 3755- 3764.

[65] DAI H N, ZHENG Z, ZHANG Y. Blockchain for Internet of Things: A survey[J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[66] LU Y, HUANG X, ZHANG K, et al. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4298-4311.

[67] QIU X, LIU L, CHEN W, et al. Online deep reinforcement

learning for computation offloading in blockchain- empowered mobile edge computing[J]. IEEE Transactions on Vehicular Technology, 2019, 68(8): 8050-8062.

[68] BTC.BTC Relay Documentation[EB/OL].[2020-12-29].https://btcrelay.readthedocs.io/en/latest/frequenlyaskedqu-estions.html.

[69] POONJ B. Plasma: ScalableautonomoussmartconG tracts[EB/OL]. [2017-8-11]. https://www.plasma.io/plasGmaGdeprecated. pdf.

[70] ETHHUB. ZK-Rollups[EB/OL].[2020-12-29].https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-rollups.

[71] SINGH A, CLICK K, PARIZI R M, et al. Sidechain technologies in blockchain networks: An examination and state-of-the-art review[J]. Journal of Network and Computer Applications, 2020, 149: 102471.

[72] KAPPOS G, YOUSAF H, PIOTROWSKA A, et al. An empirical analysis of privacy in the lightning network[C]// Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I 25. Springer Berlin Heidelberg, 2021: 167-186.

[73] NETWORK R. What is the raiden network? [EB/OL]. [2018-12-22].https://raiden. network/101. html.

[74] DZIEMBOWSKI S, ECKEY L, FAUST S, et al. Perun: Virtual payment hubs over cryptocurrencies[C]//2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019: 106-123.

[75] EGGER C, MORENO-SANCHEZ P, MAFFEI M.Atomic multi-channel updates with constant collateral in bitcoin-compatible payment-channel networks[C]//Pro-ceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019: 801-815.

[76] PAN C, TANG S, GE Z, et al. Gnocchi: Multiplexed Payment Channels for Cryptocurrencies[C]//International Conference on Network and System Security. Springer, Cham, 2019: 488-503.

[77] 葛钟慧,张奕,龙宇,刘振,刘志强,谷大武.一种支持高并发的多人链下支付方案[J].计算机学报,2021,44(01):132-146.
GE Z H,ZHANG Y,LONG Y,LIU Z,LIU Z Q,GU D W. A High-Concurrency Multi-person off-chain payment scheme[J].Chinese Journal of Computers,2021,44(01): 132-146.

[78] GRUNSPAN C, PÉREZ-MARCO R. Ant routing algorithm for the lightning network[J]. arXiv preprint arXiv:1807.00151, 2018.

[79] PRIHODKO P, ZHIGULIN S, SAHNO M, et al. Flare: An approach to routing in lightning network[J]. White Paper, 2016: 144.

[80] ROOS S, MORENO-SANCHEZ P, KATE A, et al. Settling payments fast and private: Efficient decentralized routing for path-based transactions[J]. arXiv preprint arXiv:1709.05748, 2017.

[81] DONG M, LIANG Q, LI X, et al. Celer network: Bring internet scale to every blockchain[J]. arXiv preprint arXiv:1810.00037, 2018.

[82] YU R, XUE G, KILARI V T, et al. Coinexpress: A fast payment routing mechanism in blockchain-based payment channel networks[C]//2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2018: 1-9.

[83] SIVARAMAN V, VENKATAKRISHNAN S B, RUAN K, et al. High throughput cryptocurrency routing in payment channel networks[C]//17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20). 2020: 777-796.