区块链 PCN 的高效路由策略

霍如[1,2]，倪东[2]，卢华[3]，夏云峰[2]，汪硕[2,4]，黄韬[2,4]，刘韵洁[1,2,4]

（1. 北京工业大学信息学部，北京 100124；2. 网络通信与安全紫金山实验室，江苏 南京 211111；
3. 广东省新一代通信与网络创新研究院，广东 广州 510663；4. 北京邮电大学网络与交换国家重点实验室，北京 100876）

摘 要：针对付费信道网络交易成功率低及网络失衡问题，提出区块链付费信道网络高效路由策略。该策略根据业务类型及业务优先级为高优先级业务建立专用付费信道，并将常规业务划分为多个交易单元，通过信道均衡选路算法为各交易单元选路，减少链上交易次数，维持付费信道的长时间稳定性运行，提高交易成功率。为了避免多个交易同时使用某一链路导致资金暂时性短缺、信道不可用，设计付费信道网络交易排队机制。该机制通过计算交易到达节点与下一跳节点之间的托管金额，建立交易的转发规则，对于排队阈值内无法进行资金注入的节点，设计信道均衡选路算法为其计算新的转发路径。仿真结果表明，所提策略可以提高交易成功率并实现付费信道网络均衡。

关键词：区块链；付费信道网络；交易单元；差异化路由；信道均衡

中图分类号：TP311.13，TP393.0

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021113

Efficient routing strategy of blockchain-based payment channel network

HUO Ru[1,2], NI Dong[2], LU Hua[3], XIA Yunfeng[2], WANG Shuo[2,4], HUANG Tao[2,4], LIU Yunjie[1,2,4]

1. Information Department, Beijing University of Technology, Beijing 100124, China
2. Purple Mountain Laboratories, Nanjing 211111, China
3. Guangdong Communications & Networks Institute, Guangzhou 510663, China
4. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: In order to solve the problems of the low transaction success rate and network imbalance of the payment channel network, an efficient routing strategy of blockchain-based payment channel network was proposed. This strategy established a dedicated payment channel for the high-priority services according to the service type and service priority, and divided the conventional business into multiple transaction unit. Furthermore, a channel balanced routing algorithm was designed to route each transaction unit, which could reduce the number of transactions on the blockchain and maintain long-term stable operation of the off-chain payment channel, as well as improve the transaction success rate. In addition, in order to avoid the temporary shortage of funds and unavailability of channels due to a certain link occupied by multiple transactions simultaneously, a transaction queuing mechanism in the payment channel network was designed. This mechanism established the forwarding rules for transactions by calculating the escrow amount between the node that transactions arrived and the next hop node, where the channel balanced routing algorithm was used to calculate the new forwarding path for the nodes that could not carry out capital injection within the queuing threshold. The simulation results show that the proposed strategy could improve the transaction success rate and realize the equilibrium of the payment channel network.

Keywords: blockchain, payment channel network, transaction unit, differentiated routing, channel equalization

收稿日期：2021−02−22；**修回日期**：2021−04−23

通信作者：卢华，luhua@gdcni.cn

基金项目：2020 年工业互联网创新发展工程基金资助项目（工业互联网标识资源搜索系统）；2019 年工业互联网创新发展工程基金资助项目（创新型工业互联网标识解析系统）

Foundation Items: The MIIT of China 2020 (Identification Resources Search System for Industrial Internet of Things), The MIIT of China 2019 (Innovative Identification and Resolution System for Industrial Internet of Things)

1　引言

区块链技术本质上是一种基于分布式对等网络的基础架构和计算范式，具有去中心化、不可篡改、可追溯、匿名性和透明性五大特征，这些特征为构建安全可信的分布式交易环境提供了良好的契机[1-3]。然而，受严格共识过程和签名认证机制的约束，区块链的吞吐量很低且可扩展性差。比特币的吞吐量为 3~7 笔/秒交易，而以太坊的吞吐量大约是比特币的两倍[4-5]。在全球电子支付场景中，Visa 或其他集中式支付服务提供商每秒可以处理数千笔交易，这是目前的区块链技术无法企及的。随着微交易的出现，区块链的可扩展性问题被进一步放大，这种交易通常对实时性要求较高。此外，区块链账本收取的费用可能高于交易金额，这对交易双方来说通常不能接受。

付费信道可以解决上述挑战，方法是在 2 个用户之间建立付费信道，并在信道中托管一定的资金，将交易从链上转移到链下，避免了链上共识和确认的时延[6]。付费信道只有开启和关闭时，才会在区块链中写入交易，链下交易可以在用户之间频繁执行，不需要上链。因此提高了交易效率、可扩展性和吞吐量。

在每个交易发送方与接收方之间建立付费信道会产生一定成本，对于不存在直接付费信道的用户之间可以通过中间节点转发交易。连接不同用户的付费信道共同构成了付费信道网络（PCN, payment channel network）[7]。

PCN 和传统网络的根本区别在于存在节点的资金消耗。节点之间的交易通过中间节点转发，中间节点一侧资金的输入意味着另一侧资金的输出。如果中间节点的输出侧资金耗尽，它将无法启动该方向的任何交易或充当交易的中间节点。人们可以通过链上对资金耗尽节点的资金补充来解决这个问题，但该过程涉及复杂的链上共识和签名认证，影响链下的交易进程和交易成功率[8]。为此如何维持链下付费信道的长时间稳定性运行、减少链上交易次数是保证 PCN 高吞吐量稳定运行的重要因素。

现阶段提升 PCN 吞吐量的主要策略有业务路由优化策略和链下信道再均衡策略 2 种。路由优化策略指设计路由策略让业务沿着资金足够或增加信道平衡的路径传输。链下信道再均衡策略指在 PCN 出现信道失衡时进行全网资金调整，为资金不足的节点注入资金，进而实现 PCN 均衡。

在 PCN 路由优化策略研究方面，Sivaraman 等[7]提出了一种 Spider 算法来解决最短路径算法选路引起的资金耗尽问题。该策略利用了互联网包交换的思想将交易划分为交易单元，并使用多路径传输协议实现高吞吐量路由，同时设计多路径拥塞控制协议确保信道的均衡使用。Yu 等[9]提出了一种 CoinExpress 新型分布式动态路由机制。该机制设计了基于网络流和并发流的 PCN 路由模型，在保证交易路由的同时保证交易时延。Zhang 等[10]提出了一种分布式稳健支付路由协议 RobustPay 来抵抗事务失败，实现了 PCN 的稳健性、高效性和分布式，同时修改了闪电网络的 HTLC 协议，使其适应强大的支付路由协议。Lin 等[11]提出了一种 FSTR 路由算法，该算法基于资金倾斜度进行交易路径选择，在减小资金倾斜度的同时提高交易成功率。Pavel 等[12]提出了一种混合路由算法 Flare，该算法通过设置网络中的信标节点来获取网络的本地视图，本地节点和信标节点的结合使节点最大限度地减少路由状态，同时以高概率查找到任意给定节点的路由。

在 PCN 链下信道再均衡策略研究方面，Pickhardt 等[13]提出了一种闪电网络的链下信道再均衡算法，通过对网络上循环路径的资金调整实现信道再均衡。Mercan 等[14]提出了一种物联网场景下的 PCN 设计，通过在网络上使用通用权重策略来保持信道均衡，并针对不平衡的支付方案，为每个物联网设备设置多个连接来提高交易成功率。

目前，对路由优化策略的研究大多只考虑交易成功率，如文献[9-12]，这些研究未考虑交易后的信道失衡问题，导致网络的平衡度迅速下降，而且一个交易请求到达时立即原子性地路由整笔交易。当付费信道缺少足够的资金时，即使信道在短时间内会进行资金补充，也会导致交易立即失败。其对金额较大的交易影响尤其严重。目前，大多的链下信道再均衡策略采用全网均衡的方式，如文献[13-14]，这些研究可以很好地解决 PCN 吞吐量低的问题，但在逐年扩大的 PCN 中进行全网均衡将影响正常的交易进程，这对于实时性要求较高的电子支付类业务是无法接受的。最重要的是，目前主要是针对 2 种策略的单独研究，很少考虑 2 种策略的结合，业务路由优化策略和链下信道再均衡策略的割裂导致算法的性能优化受限。最后，现阶段的 PCN 对所有的业务采用统一的选路策略，没有考虑针对不同的业务类型设置优先级，对于服务质量要求较

高的业务无法实现服务质量保障。

基于上述问题，本文提出 PCN 的高效路由策略（ERS_PCN, efficient routing strategy of block-chain-based PCN）。该策略根据业务类型及业务优先级为高优先级业务建立专用付费信道，并将常规业务划分为多个交易单元，通过信道均衡选路算法为各交易单元选路，在路由层面上实现信道均衡，减少链上交易次数，维持付费信道的长时间稳定性运行，提高交易成功率。本文的主要贡献如下。

1) 设计差异化专用信道服务算法。根据交易类型和交易优先级为高优先级交易建立专用付费信道，来保证交易的服务质量。

2) 设计多路径转发算法。将交易拆分为独立的交易单元，采用多路径传输的方式独立传送这些单元。

3) 设计信道均衡选路算法。针对请求计算一定数量的候选路径，计算每一条候选路径路由后的网络基尼系数，并选择使网络基尼系数最低的路径转发交易。

4) 设计 ERS_PCN 策略。该策略由差异化专用信道服务算法、多路径转发算法、信道均衡选路算法 3 个部分组成。

5) 采用网络基尼系数、交易成功率作为评价指标，构建 PCN 拓扑与业务模型进行仿真，验证算法优越性。

2 系统模型

为了设计 ERS_PCN 策略，本节从平台和算法 2 个层面考虑来设计系统模型。其中，平台模型包括 PCN 应用分层模型、区块链模型和 PCN 模型，主要为 ERS_PCN 策略的实现提供底层支撑平台；算法模型包括 K 路径算法模型和 PCN 基尼系数模型，主要为 ERS_PCN 策略的实现提供算法支撑。PCN 与区块链网络之间存在交互关系，本节首先设计 PCN 应用分层模型，该模型由物理层、区块链层、PCN 层和应用层组成，其中区块链层和 PCN 层是模型的核心。考虑到区块链层是支撑 PCN 安全稳定运行的重要因素，因此本节进一步对区块链模型进行了介绍。同时，为了便于后续算法研究的量化，本节提出了 PCN 模型，对 PCN 层进行模型抽象。最后介绍了 K 路径算法模型和 PCN 基尼系数模型，为 ERS_PCN 策略中的多交易单元多路径传输和评价信道是否均衡提供理论参考依据。

2.1 PCN 应用分层模型

参考现有的通用区块链应用分层模型[15]，本文设计了如图 1 所示的 PCN 应用分层模型，该模型分为 4 层，自下而上分别为物理层、区块链层、PCN 层和应用层。考虑到应用与区块链网络及 PCN 的交互关系，4 层模型主要在传统通用区块链应用分层模型基础上进行了 PCN 层的增加和各层的改进，以适用于本文方法的应用与实现，其中 PCN 层处在应用层和区块链层之间，便于对上支持支付类应用，对下与区块链底层技术进行交互。

1) 物理层

物理层是硬件层，它由个人计算机、云服务器、小型服务器、大型服务器等硬件设备组成。该层为区块链层提供丰富的计算资源与存储资源，可以在众多平台上挖掘不同硬件的计算能力与存储能力，加快上层的共识进程，减小链上共识时间。

2) 区块链层

区块链是通过区块链接在一起的有序记录的列表，该层利用分布式共识算法生成和更新数据，并利用对等网络进行节点间的数据传输，结合密码学原理等技术保证存储数据不可篡改，支撑 PCN 层的稳定运行，保证 PCN 层交易的链上最终一致性。

3) PCN 层

PCN 层是 PCN 应用分层模型的核心，主要完成应用层下发的付费业务，完成与区块链层的交互，将交易从链上转移到链下，避免了链上共识和确认的时延，保证付费交易的安全性与实时性。

4) 应用层

应用层为众多付费应用的集合，这些应用通过接入网关接入 PCN 层，实现跨境支付、知识付费等电子支付业务。

2.2 区块链模型

区块链主要解决 PCN 资金交易的信任和安全问题，本文主要利用区块链的 4 种技术来支撑 PCN 的安全稳定运行。

1) 分布式账本

交易记账由分布在不同地方的多个节点共同完成，每一个节点都记录完整的交易副本，共同参与监督交易的合法性。PCN 链下资金交易结束，需上链存储到分布式账本进行交易的记录。

2) 非对称加密和授权技术

存储在区块链上的交易信息是公开的，但是交

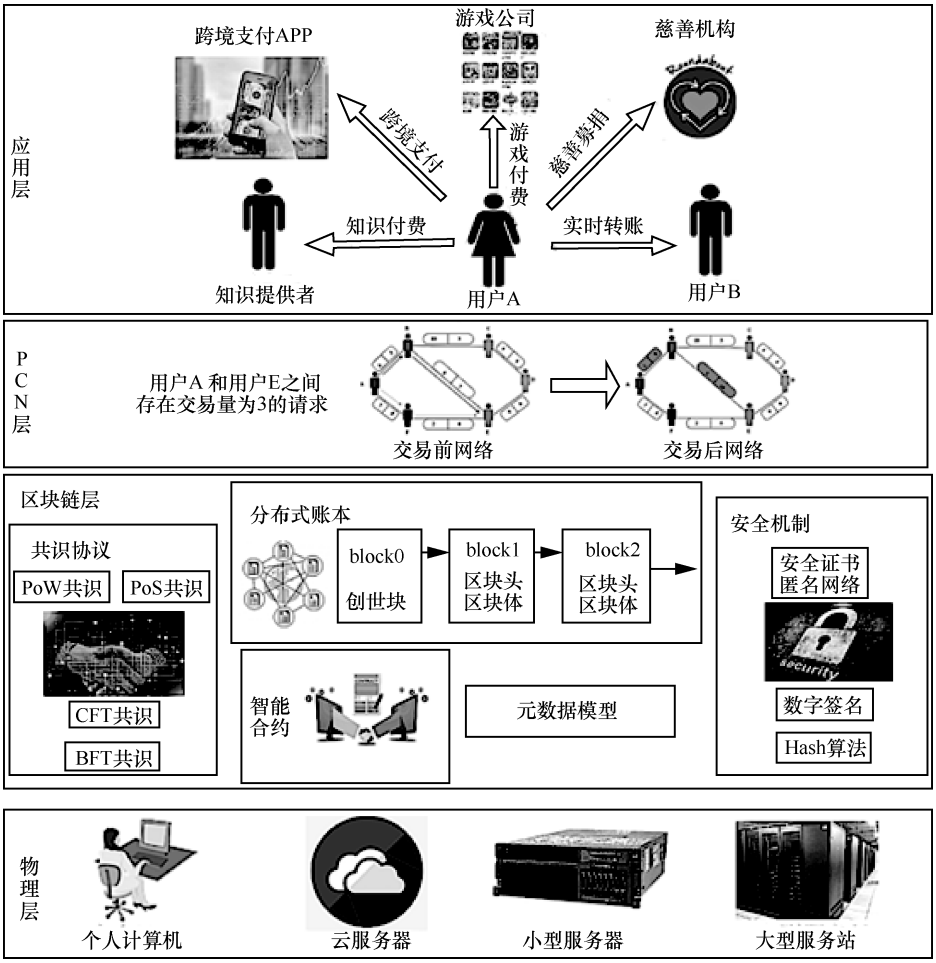


图 1　PCN 应用分层模型

易账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问到，从而保证了交易信息的安全和个人的隐私。

3) 共识机制

共识机制通过特殊节点的投票，完成对交易的验证和确认；对一笔交易，如果利益不相干的若干个节点能够达成一致，则可以认为全网对此达成共识，即由不同节点组成的系统之间依赖一个制度来维护系统的数据一致性。PCN 链下资金交易结束，在链上达成共识后方可进行交易上链。

4) 智能合约

智能合约是基于可信不可篡改的数据，自动化执行的一些预先定义好的规则和条款。PCN 链下资金交易结束，需通过智能合约实现交易的上链逻辑，进行 PCN 与区块链的交互。

2.3　PCN 模型

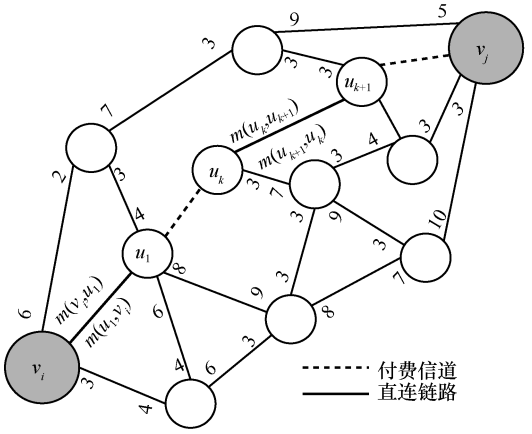
假设拓扑 $G=(N,E)$ 是一个 PCN，其中，N 表示整个网络中的节点数，即 PCN 中的所有参与者个数，$N\geqslant 2$；E 表示整个网络中的链路集合，即 PCN 中的所有付费信道。假设节点 v_i 和节点 v_j 为 G 中存在付费信道的 2 个节点，信道 $\mathrm{Path}(v_i,v_j)$ 为链路 $e_1,\cdots,e_l$ 的集合，l 为 $\mathrm{Path}(v_i,v_j)$ 的链路个数。当 l=1 时，v_i 和 v_j 之间存在直连链路。为了方便说明，本文假设 $l\geqslant 3$。$e_k=(u_k,u_{k+1})$ 表示 $\mathrm{Path}(v_i,v_j)$ 路径上中间节点 u_k 与 u_{k+1} 之间的直连链路，$1\leqslant k\leqslant l-1$；$m(u_k,u_{k+1})$ 表示节点 u_k 到节点 u_{k+1} 方向的可流通资金。$\mathrm{Path}(v_i,v_j)$ 示意如图 2(a)所示。此外，将 $\mathrm{Max}M_{\mathrm{Path}(v_i,v_j)}$ 定义为 $\mathrm{Path}(v_i,v_j)$ 的最大可流通资金，计算式为

$$\mathrm{Max}M_{\mathrm{Path}(v_i,v_j)}=\min(m(v_i,u_1),\cdots,m(u_k,u_{k+1}),\cdots,m(u_{l-1},v_j)) \quad (1)$$

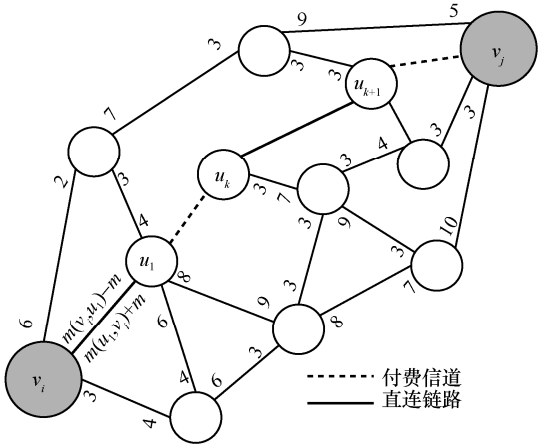
其中，$\min(\cdots)$ 表示取最小值函数。

假设在时刻 t，节点 v_i 到节点 v_j 存在交易需求

$\mathrm{trans}_t(v_i,v_j,m)$，其中 m 表示交易金额。如果该信道上 $\mathrm{Max}M_{\mathrm{Path}(v_i,v_j)} \geqslant m$，则信道 e_k 交易后节点 u_k 到节点 u_{k+1} 方向的可流通资金变为 $m(u_k,u_{k+1})-m$，节点 u_{k+1} 到节点 u_k 方向的可流通资金变为 $m(u_{k+1},u_k)+m$，路径上其他链路的资金流动情况相同，交易后的示意如图 2(b)所示。



(a) Path(v_i,v_j)示意



(b) 交易后 Path(v_i,v_j)示意

图 2　PCN 模型示意

2.4　K 路径算法模型

路由技术旨在发现业务的源、目的节点之间的合适路径[16]。其中，最短路径算法指寻找网络中两节点之间的最短路径，是目前网络路由研究中较常用的基础路由算法。K 最短路（KSP, K shortest paths）算法[17-18]是在最短路径算法基础上的升级。与最短路径算法不同，KSP 算法寻找源节点与目的节点之间的多条路径，并组成最短路径集合，以满足用户对不同路径的多样化需求。

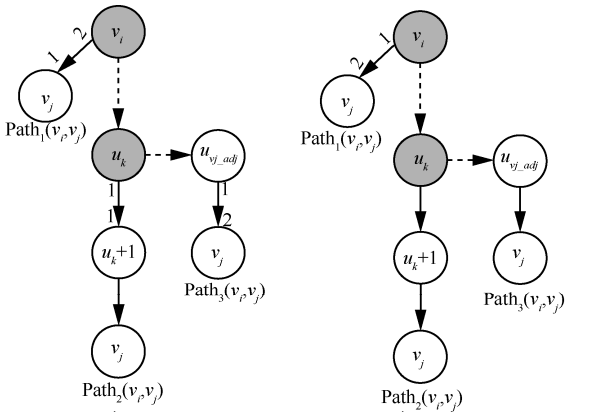
本文利用 KSP 算法的思路，并根据不同的基础路由算法设计新的 K 路径算法，如 K 最短路径算法的基础路由算法为最短路径算法。假设一个业务请求的源、目的节点分别为 v_i 和 v_j，K 路径算法可分为两部分。

1) 利用基础路由算法算出首条路径 $\mathrm{Path}_1(v_i,v_j)$，然后在此基础上依次算出其他的 K-1 条路径。

2) 在求 $\mathrm{Path}_{k+1}(v_i,v_j)$ 时（$1<k<K$），将 $\mathrm{Path}_k(v_i,v_j)$ 上除了目的节点外的所有节点都视为背离节点，并根据基础路由算法计算每个背离节点到目的节点的路径，再与之前的 $\mathrm{Path}_k(v_i,v_j)$ 上源节点到背离节点的路径连接，构成候选路径。

采用合适的 K 路径算法，在各候选路径上进行独立的交易单元传输可以分散高金额交易到多个付费信道中，从而达到提供交易成功率的目的。

假设 K=3，节点 v_i 与 v_j 之间存在交易量为 3 的请求，节点 v_i 与 v_j 的 K 路径选路结果示例如图 3(a)所示。其中，$\mathrm{Path}_1(v_i,v_j)$ 与 $\mathrm{Path}_2(v_i,v_j)$ 之间的偏离节点为 v_i，$\mathrm{Path}_2(v_i,v_j)$ 与 $\mathrm{Path}_3(v_i,v_j)$ 之间的偏离节点为 u_k。从图 3(a)可以看出，3 条路径的最大可流通资金均无法满足需求，将交易请求平均分散到 3 条候选路径可交易成功，结果如图 3(b)所示。



(a) K=3时，v_i与v_j之间路径示意　(b) K=3时，v_i与v_j之间转账结果示意

图 3　K 路径算法示例

2.5　PCN 基尼系数模型

基尼系数[19]是根据洛伦兹曲线判断一项内容分配公平程度的指标。本文采用该指标评价 PCN 的均衡程度。

假设用户在网络中实际托管金额曲线与托管金额绝对平等曲线之间为区域 A，实际托管金额曲线与坐标轴之间为区域 B，如图 4 所示。区域 A 的

面积除以区域A与区域B的面积和表示网络不均衡程度，如式(2)所示，称之为 PCN 基尼系数。

$$\mathrm{Gini}_{\mathrm{G\_PCN}}=\frac{S_{\mathrm{A}}}{S_{\mathrm{A}}+S_{\mathrm{B}}} \tag{2}$$

其中，S_{A} 表示区域 A 的面积，S_{B} 表示区域 B 的面积。

如果区域 A 的面积为 0，即 $\mathrm{Gini}_{\mathrm{G\_PCN}}=0$，表示网络完全均衡；如果区域 B 的面积为 0，则 $\mathrm{Gini}_{\mathrm{G\_PCN}}=1$，此时网络绝对不均衡。

式(2)可以从物理意义上直观地表示网络基尼系数，但不具有实际可操作性。为了便于在实际问题中更好地运用该指标直接度量 PCN 的不平衡程度，此处从数学意义上描述网络基尼系数，并证明该描述方式的正确性，PCN 基尼系数的数学表达形式为[20]

$$\mathrm{Gini}_{\mathrm{T\_PCN}}=\frac{\Delta}{2\mu} \tag{3}$$

其中，μ 表示网络托管金额均值，Δ 表示基尼平均差。Δ 可由式(4)计算得到[20]。

$$\Delta=\frac{\sum_{i=1}^{2M}\sum_{j=1}^{2M}|m_j-m_i|}{4M^2} \tag{4}$$

其中，$|m_j-m_i|$是任何一个付费信道中的两用户托管金额差值的绝对值，M 表示 PCN 的总付费信道个数。

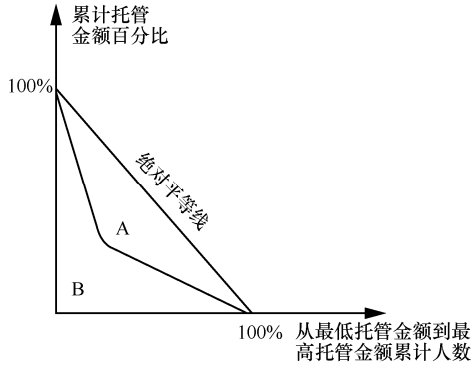


图 4　PCN 洛伦兹曲线与基尼系数

已知 $\mathrm{Gini}_{\mathrm{T\_PCN}}=\frac{\Delta}{2\mu}=2S_{\mathrm{A}}$ [20]，由图 4 可知，$S_{\mathrm{A}}+S_{\mathrm{B}}=\frac{1}{2}$，代入式(2)得到 $\mathrm{Gini}_{\mathrm{G\_PCN}}=2S_{\mathrm{A}}$。因此，可以得出 $\mathrm{Gini}_{\mathrm{G\_PCN}}=\mathrm{Gini}_{\mathrm{T\_PCN}}$，证明式(3)即可作为 PCN 基尼系数的数学表达形式，将式(4)代入式(3)，进一步整理，得到 PCN 基尼系数最终的数学表达形式为

$$\mathrm{Gini}_{\mathrm{G}}=\frac{\sum_{i=1}^{2M}\sum_{j=1}^{2M}|m_j-m_i|}{8M^2\mu} \tag{5}$$

3　策略设计与实现

PCN 高效路由策略根据业务类型及业务优先级为高优先级业务建立专用付费信道，并将常规业务划分为多个交易单元，通过信道均衡选路算法为各交易单元选路，减少链上交易次数，维持付费信道的长时间稳定性运行，提高交易成功率，该策略由差异化专用信道服务算法、多路径转发算法和信道均衡选路算法 3 个部分组成。

3.1　差异化专用信道服务算法

差异化专用信道服务算法针对不同的业务类型建立不同的专用信道，保证高优先级业务获得 $\mathrm{trans}_t(v_i,v_j,m,\mathrm{type},\mathrm{pri})$ 更好的服务质量。对于高优先级用户，针对其不同的业务类型建立专用信道提供差异化服务。本文将交易类型分为高金额业务、低时延业务、高可靠业务、常规业务几类。对除了常规业务以外的业务建立专用信道保证交易的服务质量。差异化专用信道服务算法可简述为：首先，判断交易的业务类型及优先级；其次，决定业务的交易路径。具体算法流程如算法 1 所示。

算法 1　差异化专用信道服务算法

输入　$\mathrm{trans}_t(v_i,v_j,m,\mathrm{type},\mathrm{pri})$

1) 收到一个交易 $\mathrm{trans}_t(v_i,v_j,m,\mathrm{type},\mathrm{pri})$；

2) if（type=常规业务）then

3)　按照多路径转发算法和信道均衡选路算法选择交易路径；

4) elseif（type=高金额业务）then

5)　建立专用高金额付费信道执行交易；

6) elseif（type=低时延业务）then

7)　建立专用低时延付费信道执行交易；

8) else　建立专用高可靠付费信道执行交易；

9) end if

3.2　多路径转发算法

多路径转发算法在交易发送方将交易拆分成一系列独立路由的交易单元，每个交易单元都转移一笔以最大交易单元（TRANS_UINT, transaction unit）为边界的金额。由于使用独立的密钥创建每个交易单元，拆分交易并不会影响交易的安全性。当交易接收方接收并确认交易单元时，发送方可以选择性地仅显示已确认交易单元的密钥。交易发送

方在交易过程中将收到通知，告知他们已完成了多少交易单元，发送方可以选择取消未完成的交易单元或在区块链上重试。多路径转发算法简述如下。首先，计算交易单元个数为

$$\text{num}_{\text{Tunit}} = \text{RoundU}\left(\frac{m}{\text{MTU}}\right) \tag{6}$$

其中，RoundU(…) 表示向上取整函数，MTU 表示交易单元大小，m 表示交易金额。

其次，划分交易单元，并对各交易单元加密。然后，使用 K 路径算法计算各交易单元的转发路径，计算转发路径条数为

$$\text{NUM}_{\text{path}}(\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri})) = \min(\text{num}_{\text{Tunit}}, \text{NUM}_{\text{path}}(v_i, v_j)) \tag{7}$$

最后，沿着各路径独立转发交易单元。具体算法流程如算法 2 所示。

算法 2 多路径转发算法

输入 $\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri})$，MTU，K 路径算法，交易签名策略

1) 收到一个交易请求 $\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri})$；

2) if（$m \leqslant$ MTU）then

3) 按照网络原有路由策略路由整笔交易；

4) else 计算 v_i 到 v_j 的所有可转发路径个数 $\text{NUM}_{\text{path}}(v_i, v_j)$；

5) 按照式(4)计算交易单元个数 $\text{num}_{\text{Tunit}}$；

6) 按照式(5)计算转发路径个数 $\text{NUM}_{\text{path}}(\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri}))$；

7) end if

8)if（$\text{NUM}_{\text{path}}(\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri})) = \text{num}_{\text{Tunit}}$）then

9) 将 $\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri})$ 划分为 $\text{num}_{\text{Tunit}}$ 个交易单元；

10) 按照交易签名策略对 $\text{num}_{\text{Tunit}}$ 个交易单元签名；

11) $K = \text{num}_{\text{Tunit}}$；

12) 按照 K 路径算法同时转发各交易单元；

13) else if（$\text{NUM}_{\text{path}}(\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri})) < \text{num}_{\text{Tunit}}$）then

14)按照交易签名策略对 $\text{NUM}_{\text{path}}(\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri}))$ 个交易单元签名；

15) $K = \text{NUM}_{\text{path}}(\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri}))$；

16) 按照 K 路径算法同时转发 $\text{NUM}_{\text{path}}(\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri}))$ 个交易单元；

17) $\text{num}_{\text{Tunit}} -= \text{NUM}_{\text{path}}(\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri}))$，返回步骤 13)；

18) else 按照交易签名策略对 $\text{num}_{\text{Tunit}}$ 个交易单元签名；

19) $K = \text{num}_{\text{Tunit}}$；

20) 按照 K 路径算法同时转发 $\text{num}_{\text{Tunit}}$ 个交易单元；

21) end if

22)end if

3.3 信道均衡选路算法

在一个交易请求到达 PCN 时，为该请求计算一定数量的候选路径，信道均衡选路算法会计算每一条候选路径路由后的网络基尼系数，并选择网络基尼系数最小的路径转发交易。如果找不到可行的路径，则路由失败。信道均衡选路算法流程可整理为：首先，计算 M 条候选路径；其次，计算通过各候选路径路由后的网络的基尼系数；最后，选择使网络基尼系数最小的路径作为最终的交易路径。具体算法流程如算法 3 所示。

算法 3 信道均衡选路算法

输入 $\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri})$，候选路径个数 M，K 路径算法

1) 收到一个交易请求 $\text{trans}_t(v_i, v_j, m, \text{type}, \text{pri})$；

2) 计算 v_i 到 v_j 的所有可转发路径个数 $\text{NUM}_{\text{path}}(v_i, v_j)$；

3) if ($\text{NUM}_{\text{path}}(v_i, v_j) < M$) then

4) $M = \text{NUM}_{\text{path}}(v_i, v_j)$；

5) K=M，根据 K 路径算法计算 M 条候选路径，得到候选路径集合为 $U_{\text{path}} = \{\text{Path}_1, \cdots, \text{Path}_i, \cdots, \text{Path}_M\}$；

6)i=0；

7) for（i<M）then

8) 利用式(3)计算 Path_i 路由后的网络基尼系数 $\text{Gini}_{\text{G\_Path}_i(af)}$；

9) i=i+1，返回步骤 7)；

10) 计算 $\min(\text{Gini}_{\text{G\_Path}_1(af)} \cdots \text{Gini}_{\text{G\_Path}_M(af)})$；

11) 选择 $\min(\text{Gini}_{\text{G\_Path}_1(af)} \cdots \text{Gini}_{\text{G\_Path}_M(af)})$ 对应的路径 Path_k 作为最终交易路径。

3.4 PCN 高效路由策略实现

根据算法 1~算法 3，本节设计了 ERS_PCN 策

略的具体实现，流程如图 5 所示。对于 t 时刻到来的一个交易请求 $\text{trans}_t(v_i,v_j,m,\text{type},\text{pri})$，首先根据 type 和 pri 判断交易是否为常规业务，如果不是，则按照算法 1 进行交易的路由与转发。如果 $\text{trans}_t(v_i,v_j,m,\text{type},\text{pri})$ 为常规业务，则使用算法 2 计算转发路径个数为 $\text{NUM}_{\text{path}}(\text{trans}_t(v_i,v_j,m,\text{type},\text{pri}))$。计算候选路径个数如式(8)所示。

$$\text{NUM}_{\text{Cpath}}(\text{trans}_t(v_i,v_j,m,\text{type},\text{pri})) = \min(\text{mutli}\cdot \text{NUM}_{\text{path}}(\text{trans}_t(v_i,v_j,m,\text{type},\text{pri})),\text{NUM}_{\text{path}}(v_i,v_j)) \tag{8}$$

其中，$\text{mutli}\geqslant 1$。为了实现更好的信道均衡，PCN 的连通度越高，mutli 应越大。

然后，计算 $\text{NUM}_{\text{Cpath}}(\text{trans}_t(v_i,v_j,m,\text{type},\text{pri}))$ 条候选路径的路由后网络基尼系数。对计算得到的网络基尼系数进行升序排序整理，选择排名在前 $\text{NUM}_{\text{path}}(\text{trans}_t(v_i,v_j,m,\text{type},\text{pri}))$ 条的路径作为本次交易路径。

在 ERS_PCN 策略中，为了避免多个交易同时使用某一链路导致资金的暂时性短缺，交易到达某一节点时需要计算该节点与下一跳节点之间的托管金额是否满足交易需求，如果满足则转发至下一跳，否则交易在该节点处进行排队，并为队列中的每一笔交易设置一个时间阈值，如果在阈值范围内该节点与下一跳节点之间流入足够的资金，业务沿着原路径转发，否则以该节点为源节点，利用算法 3 为其计算新的转发路径。

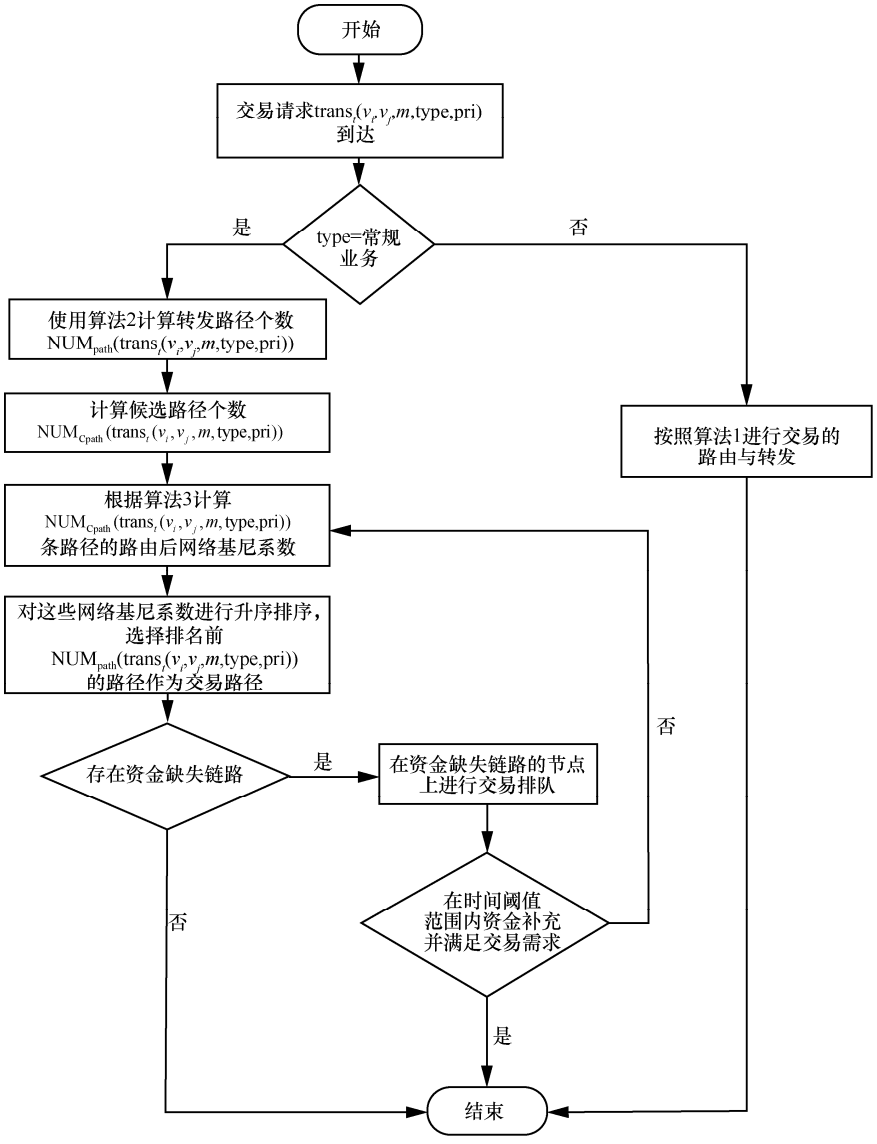


图 5　ERS_PCN 策略实现流程

4　仿真分析

为了验证所提 ERS_PCN 策略的优越性，本文利用 python 的 networkx 库模拟网络拓扑来构建实验。使用一台 Linux 服务器作为硬件运行环境，服务器采用 Centos 系统，32 GB 内存。本文分别采用 small-world 和 scale-free 这 2 个拓扑，节点个数均为 300 个，small-world 网络拓扑的节点平均度数为 4，scale-free 网络拓扑的节点平均度数为 3[21]。本节分别从交易成功率和网络基尼系数 2 个方面进行算法的仿真，并与 Dijkstra 算法[22]和 Spider 算法[7]进行了对比。其中，交易成功率指一段时间内成功交易的个数占总交易请求个数的比值。本文仿真参数设置如表 1 所示。

表 1　　仿真参数设置

参数	值
拓扑	small-world、scale-free
节点个数	300 个
基础路由算法	最短路径算法
mutli	10 倍
pri_{the}	3 级
TRANS_UINT	2 瑞波币
平均交易金额	6 瑞波币
交易排队时间	300 ms
交易平均优先级	2 级

瑞波币是 Ripple 网络[21]内的流动性代币，可以作为各类货币之间兑换的中间品。本文从 Ripple 网络收集了现实世界中的付款数据，并以瑞波币作为 PCN 中的流动代币。为此，本文检索了 2020 年 12 月 31 日发生的所有瑞波币交易，通过随机抽样从该数据集中选择交易。实验中交易数量以 120 个为步长，每秒到达 PCN 的交易个数从 120 个依次递增到 720 个，对每个交易数量进行 50 次重复实验，保证实验结果的有效性。

small-world 拓扑下每秒到达 PCN 不同交易个数时 ERS_PCN 算法与 Dijkstra 算法及 Spider 算法的交易成功率对比情况如图 6 所示，此时设置网络中各节点在各链路的平均托管金额为 10 个瑞波币。从图 6 可以看出，随着交易个数的增加，ERS_PCN 算法的交易成功率均高于 Dijkstra 算法及 Spider 算法，一直保持稳定的交易成功率，其他算法性能则会出现持续下降的趋势，交易成功率差值随着交易个数的增加而增大。这是因为 ERS_PCN 算法结合了多路径转发算法和信道均衡选路算法，将交易划分为多个交易单元，降低了因链路资金不足而交易失败的概率，同时在选路时保证信道均衡，减少了因信道失衡导致的交易失败。当交易个数为 720 个时，ERS_PCN 算法的交易成功率较 Dijkstra 算法增加了约 180%，较 Spider 算法增加了约 78%。

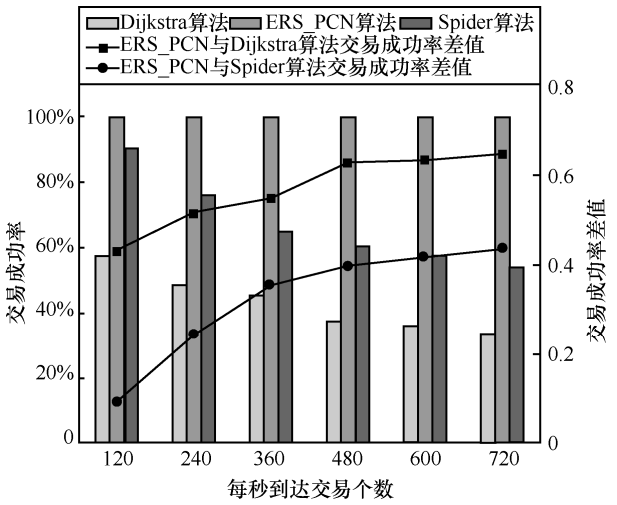


图 6　small-world 下 ERS_PCN 与 Dijkstra 算法、Spider 算法的交易成功率对比

small-world 拓扑下每秒到达 PCN 不同交易个数时 ERS_PCN 算法与 Dijkstra 算法及 Spider 算法的网络基尼系数对比情况如图 7 所示。为了保证交易全部成功，此时设置网络中各节点在各链路的平均托管金额为 100 个瑞波币。从图 7 可以看出，不同交易个数时，ERS_PCN 算法的网络基尼系数均低于 Dijkstra 算法和 Spider 算法。并且随着交易个数的增加，ERS_PCN 算法的网络基尼系数呈现较为缓慢的增长速度，3 种算法间的网络基尼系数差值的绝对值呈现逐渐增大的趋势，说明本文算法可以在一定程度上维持 PCN 信道长时间稳定运行。当交易个数为 720 个时，ERS_PCN 算法的网络基尼系数较 Dijkstra 算法减小了约 150%，较 Spider 算法减小了约 45%。

与此同时，本文采用相同的方法验证了 scale-free 拓扑下 ERS_PCN 算法的性能，结果分别如图 8 和图 9 所示。

从图 8 可以看出，ERS_PCN 算法在 scale-free 网络拓扑下仍可以表现出稳定的交易成功率。这是因为该算法实现了多路径转发算法与信道均衡选路算法的结合，减少了因链路资金不足与信道失衡

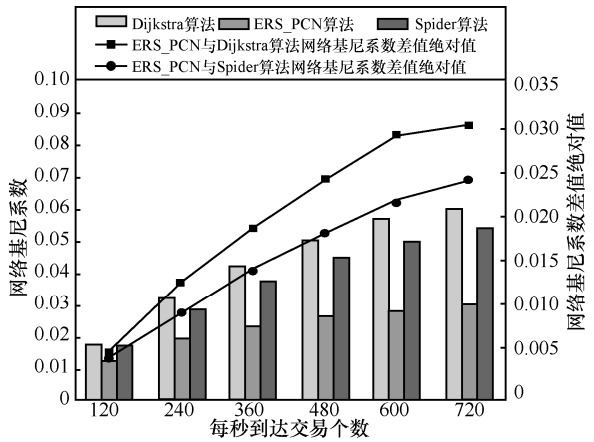


图 7　small-world 下 ERS_PCN 与 Dijkstra 算法、Spider 算法的网络基尼系数对比

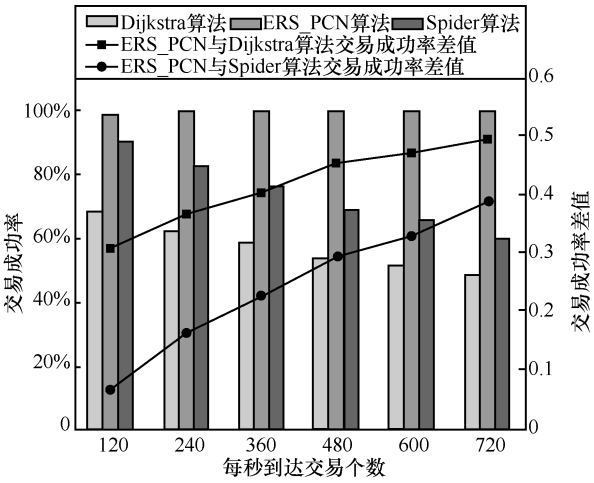


图 8　scale-free 下 ERS_PCN 与 Dijkstra 算法、Spider 算法的交易成功率对比

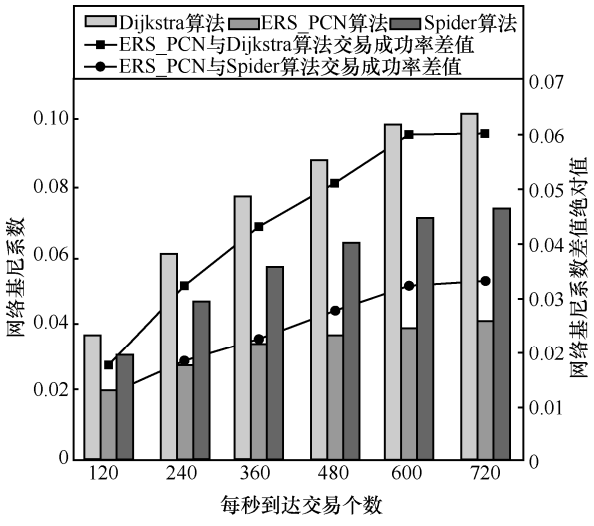


图 9　scale-free 下 ERS_PCN 与 Dijkstra 算法、Spider 算法的网络基尼系数对比

导致的交易失败。当交易个数为 720 个时，ERS_PCN 算法的交易成功率较 Dijkstra 算法增加了约 100%，较 Spider 算法增加了约 66%。从图 9 可以看出，在 scale-free 网络拓扑下 ERS_PCN 算法的网络基尼系数仍低于 Dijkstra 算法和 Spider 算法。随着交易个数的增加，ERS_PCN 算法的网络基尼系数增长较缓慢，但 3 种算法间的网络基尼系数差值的绝对值呈现逐渐增大的趋势。当交易个数为 720 个时，ERS_PCN 算法的网络基尼系数较 Dijkstra 算法减小了约 100%，较 Spider 算法减小了约 44%。

5　结束语

本文提出了一种 PCN 的高效路由策略，该策略由差异化专用信道服务算法、多路径转发算法和信道均衡选路算法 3 个部分组成。通过差异化专用信道服务算法为高优先级业务建立专用信道，保证服务质量。多路径转发算法将业务划分为 TRANS_UINT 大小的交易单元独立传输，增加交易成功率。信道均衡选路算法采用网络基尼系数作为信道是否均衡的指标进行选路，减少链上交易次数，维持付费信道的长时间稳定性运行。针对提出的方案，本文分别以交易成功率和网络基尼系数作为评价指标，在 small-world 网络和 scale-free 网络上对算法的性能进行了仿真。仿真结果表明，本文方案可以在增加交易成功率的同时，增加网络均衡性。small-world 网络下，当每秒到达网络的交易个数为 720 个时，ERS_PCN 算法的交易成功率较 Dijkstra 算法增加了约 180%，较 Spider 算法增加了约 78%；网络基尼系数较 Dijkstra 算法减小了约 150%，较 Spider 算法减小了约 45%。

参考文献：

[1] UNDERWOOD S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11): 15-17.

[2] MEMON M, HUSSAIN S S, BAJWA U A, et al. Blockchain beyond bitcoin: blockchain technology challenges and real-world applications[C]//2018 International Conference on Computing, Electronics & Communications Engineering. Piscataway: IEEE Press, 2018: 29-34.

[3] GAI R L, DU X Y, MA S Y, et al. A summary of the research on the foundation and application of blockchain technology[J]. Journal of Physics Conference Series, 2020, 1693: 012025.

[4] CHRISTIN N, SAFAVI-NAINI R. Financial cryptography and data security[M]. Berlin: Springer, 2014.

[5] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014: 1-32.

[6] MALAVOLTA G, MORENO-SANCHEZ P, KATE A, et al. Concurrency and privacy with payment-channel networks[C]//ACM SIGSAC

Conference on Computer and Communications Security. New York: ACM Press, 2017: 455-471.

[7] SIVARAMAN V, VENKATAKRISHNAN S B, RUAN K, et al. High throughput cryptocurrency routing in payment channel networks[J]. arXiv Preprint, arXiv: 1809.05088, 2018.

[8] CROMAN K, DECKER C, EYAL I, et al. On scaling decentralized blockchains[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2016: 106-125.

[9] YU R Z, XUE G L, 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. Piscataway: IEEE Press, 2018: 1-9.

[10] ZHANG Y H, YANG D J. RobustPay: robust payment routing protocol in blockchain-based payment channel networks[C]//2019 IEEE 27th International Conference on Network Protocols. Piscataway: IEEE Press, 2019: 1-4.

[11] LIN S Y, ZHANG J J, WU W G. FSTR: funds skewness aware transaction routing for payment channel networks[C]//2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE Press, 2020: 464-475.

[12] PRIHODKO P, ZHIGULIN S, SAHNO M, et al. Flare: an approach to routing in lightning network[R]. 2016.

[13] PICKHARDT R, NOWOSTAWSKI M. Imbalance measure and proactive channel rebalancing algorithm for the Lightning Network[C]//2020 IEEE International Conference on Blockchain and Cryptocurrency. Piscataway: IEEE Press, 2020: 1-5.

[14] MERCAN S, ERDIN E, AKKAYA K. Improving sustainability of cryptocurrency payment networks for IoT applications[C]//2020 IEEE International Conference on Communications Workshops. Piscataway: IEEE Press, 2020: 1-6.

[15] 朱白, 李寅. 基于区块链技术的数字图书馆场景化分层应用模型[J]. 湖北农业科学, 2020, 59(18): 127-133.
ZHU B, LI Y. The application model of digital library scene based on blockchain technology[J]. Hubei Agricultural Sciences, 2020, 59(18): 127-133.

[16] CHATTERJEE B C, SARMA N, OKI E. Routing and spectrum allocation in elastic optical networks: a tutorial[J]. IEEE Communications Surveys & Tutorials, 2015, 17(3): 1776-1800.

[17] 高松, 陆锋. K 则最短路径算法效率与精度评估[J]. 中国图象图形学报, 2009, 14(8): 1677-1683.
GAO S, LU F. The Kth shortest path algorithms: accuracy and efficiency evaluation[J]. Journal of Image and Graphics, 2009, 14(8): 1677-1683.

[18] 徐涛, 丁晓璐, 李建伏. K 最短路径算法综述[J]. 计算机工程与设计, 2013, 34(11): 3900-3906, 3911.
XU T, DING X L, LI J F. Review on K shortest paths algorithms[J]. Computer Engineering and Design, 2013, 34(11): 3900-3906,3911.

[19] LERMAN R I, YITZHAKI S. A note on the calculation and interpretation of the Gini index[J]. Economics Letters, 1984, 15(3/4): 363-368.

[20] KNIGHT J B. Explaining income distribution in less developed countries: a framework and an agenda1[J]. Oxford Bulletin of Economics and Statistics, 1976, 38(3): 161-177.

[21] MORENO-SANCHEZ P, ZAFAR M B, KATE A. Listening to whispers of ripple: linking wallets and deanonymizing transactions in the ripple network[J]. Proceedings on Privacy Enhancing Technologies, 2016(4): 436-453.

[22] YUE Y. An efficient implementation of shortest path algorithm based on Dijkstra algorithm[J]. Journal of Wuhan Technical University of Surveying & Mapping, 1999, 24(3): 209-212.

[作者简介]

霍如（1988– ），女，黑龙江哈尔滨人，博士，北京工业大学讲师，主要研究方向为未来网络、工业互联网、边缘计算、网络资源管理、区块链等。

倪东（1994– ），女，黑龙江双鸭山人，网络通信与安全紫金山实验室研究员，主要研究方向为区块链、工业互联网、标识解析技术等。

卢华（1976– ），男，江西德兴人，广东省新一代通信与网络创新研究院高级工程师，主要研究方向为核心网、新型网络架构、软件定义网络、P4 可编程、虚拟化等。

夏云峰（1988– ），男，江苏南通人，网络通信与安全紫金山实验室工程师，主要研究方向为区块链、工业互联网、标识解析技术等。

汪硕（1991– ），男，河南灵宝人，博士，北京邮电大学讲师，主要研究方向为数据中心网络、软件定义网络、网络流量调度等。

黄韬（1980– ），男，重庆人，博士，北京邮电大学教授，主要研究方向为未来网络体系架构、软件定义网络、网络虚拟化等。

刘韵洁（1943– ），男，山东烟台人，中国工程院院士，主要研究方向为未来网络技术、网络体系架构、网络融合与演进等。