

## 面向支付通道网络的多优先级资源调度算法

王小洁<sup>1</sup>, 刘子依<sup>1</sup>, 唐守泽<sup>1</sup>, 祝海琳<sup>1</sup>, 周力<sup>2</sup>, 宁兆龙<sup>1</sup>, 郭磊<sup>1</sup>

(1. 重庆邮电大学通信与信息工程学院, 重庆 400065; 2. 国防科技大学电子科学学院, 湖南长沙 410073)

**摘要:** 为了缓解不断增长的并发交易数量导致的链下支付通道拥塞问题, 提出了一种基于截止时间的优先级博弈调度 (PGSD) 算法。该算法将同向优先级调度和双向节点转发方向决策构建成 2 个相互关联的资源分配问题, 采用合作博弈对优化目标 (交易成功率和交易起始金额) 进行求解, 通过重复博弈和策略更新找到最优策略以达到动态纳什均衡, 最终实现支付通道网络 (PCN) 中交易的高效调度。基于 Kaggle 信用卡数据集的仿真结果表明, 所提多优先级调度算法具有理想的能效性能, 与其他调度算法相比, 能够实现更高的业务吞吐量和成功率。所提算法能够有效改善链下资源配置, 实现了 PCN 频繁交易的可持续性优化和高效运行。

**关键词:** 链下支付通道网络; 通道拥塞; 多优先级; 博弈调度

中图分类号: TN92

文献标志码: A

DOI: 10.11959/j.issn.1000-436x.2025022

## Multi-priority resource scheduling algorithm for payment channel networks

WANG Xiaojie<sup>1</sup>, LIU Ziyi<sup>1</sup>, TANG Shouze<sup>1</sup>, ZHU Hailin<sup>1</sup>, ZHOU Li<sup>2</sup>, NING Zhaolong<sup>1</sup>, GUO Lei<sup>1</sup>

1. School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

2. College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China

**Abstract:** To alleviate the congestion of off-chain channels caused by the increasing number of transactions and the sharing of concurrent transaction payment channels, a priority game scheduling based on deadline (PGSD) algorithm was proposed for off-chain transactions of the payment channel network (PCN). Two sub-problems of same-direction priority scheduling and bi-directional node forwarding direction decisions were constructed into two interrelated games. The optimization objectives (transaction success rate and initial transaction funds) were solved by using cooperative game theory, and the optimal strategy was found through repeated game play and adjustment of reaction strategies to achieve dynamic Nash equilibrium, ultimately realizing efficient scheduling of transactions in the PCN. Simulation results based on the Kaggle credit card dataset show that the proposed multi-priority scheduling algorithm has high energy efficiency performance, and can achieve higher transaction throughput and success rate than other scheduling algorithms. The proposed algorithm can effectively improve the off-chain resource allocation and achieve the sustainability optimization and efficient operation of PCN frequent transactions.

**Keywords:** off-chain payment channel network, channel congestion, multi-priority, game scheduling

收稿日期: 2024-09-13; 修回日期: 2025-01-23

通信作者: 周力, zhoul2035@nudt.edu.cn

基金项目: 国家自然科学基金资助项目 (No.62025105, No.62272075, No.62171449); 重庆市自然科学基金资助项目 (No.CSTB2024NSCQ-JQX0013, No.CSTB2024NSCQ-QCXMX0058); 重庆市教委科学技术研究基金资助项目 (No.KJZD-M202200601, No.KJZD-K202300608)

**Foundation Items:** The National Natural Science Foundation of China (No.62025105, No.62272075, No.62171449), The Natural Science Foundation of Chongqing (No.CSTB2024NSCQ-JQX0013, No.CTSB2024NSCQ-QCXMX0058), The Science and Technology Research Program of Chongqing Municipal Education Commission (No.KJZD-M202200601, No.KJZD-K202300608)

## 0 引言

区块链是一种分布式加密货币技术<sup>[1]</sup>, 推动了从集中式网络架构到去中心化网络架构的范式转变<sup>[2]</sup>, 促进了互不信任各方之间的可信合作<sup>[3-4]</sup>。但区块链的吞吐量较差<sup>[5]</sup>, 结算时延较高, 面临着可伸缩性挑战<sup>[6]</sup>。这种可伸缩性挑战的根源在于底层共识协议的低效性, 每个交易必须耗费几分钟到几小时并经过完全共识才能被确认<sup>[7]</sup>。这种大时延降低了区块链在时敏敏感型应用中的服务质量。因此, 支付通道网络 (PCN, payment channel network) 应运而生, 成为解决区块链可伸缩性问题的一种可靠方式。PCN 是一个由加密货币用户和支付渠道组成的链下交易网络<sup>[8]</sup>。它允许没有直接支付通道的用户在中间用户的帮助下转移支付。然而, 在实现区块链可扩展性的同时, 链下交易又面临着通道容量有限和并发交易等挑战<sup>[9]</sup>, 极易造成链下支付通道拥塞问题。

由于支付通道容量有限, 随着通道两端交易流量的不平衡, 通道的平衡会逐渐倾斜<sup>[10]</sup>, 通道容量可能会因为一端的交易流量过大而耗尽<sup>[11]</sup>。相比于采用链上操作来重新平衡耗尽的通道, 启动链下循环交易来恢复 PCN 的通道平衡状态能减少区块链关闭和重新打开通道的负担和成本<sup>[12]</sup>。当通道一侧的容量耗尽时, PCN 用户可以采用多种方式转移费用以补充通道容量, 从而有效地缓解了支付通道枯竭的问题, 提高了 PCN 的弹性和稳定性。然而当交易频繁并发时, 节点的交易处理能力和交易转发能力因交易请求过多而达到极限, 同样会导致通道拥塞, 降低交易效率<sup>[13]</sup>。因此, 为了提高交易效率, 需要充分优化节点的交易调度效率, 进而提升 PCN 的网络吞吐量<sup>[14]</sup>。

为了实现 PCN 中的通道拥塞控制, 优化交易调度效率, 学术界和工业界分别在路由机制、业务流调度、拥塞控制协议等方面开展了一些工作。文献<sup>[15]</sup>提出了一种快速路由机制, 该机制可以通过找到其他可用的路由路径来传输过载业务, 解决部分支付渠道拥堵问题。但是当整个网络拥塞时, 该机制会带来高开销。文献<sup>[16]</sup>提出了一种多路径调度方法, 该方法通过不同的路由路径发送交易以应对交易失败问题, 但会产生额外的交易负载。文献<sup>[17]</sup>探索了一种名为 Spider 的新型多路径交易调度方法, 基本思想是将交易拆分为几个部分, 并通过多

个路由路径发送。该方法开发了一种拥塞控制算法来控制为每条路径分配的交易单元数量, 可实现支付渠道金额的高利用率, 但在拥挤网络中交易时延会更高, 且会导致业务时延和速率抖动, 从而使网络性能不可预测。文献<sup>[18]</sup>设计了一个具有拥塞控制的路由协议, 每个通道在本地保持一个拥塞因子, 节点通过考虑拥塞因子来确定路由路径。然而, 这些研究大部分没有从根本上提高拥塞节点的利用效率, 而是平衡了向其他可用交易路径的交易。此外, 交易路径增多可能会增加敏感信息泄露的风险, 并导致安全问题。

本文考虑了设置多优先级来提高中间节点的转发效率, 解决 PCN 的交易调度问题。解决这一问题存在如下 3 个挑战。1) 优先级分配空间大。交易的优先级分配取决于路由路径上的节点数和每个节点的优先级等级。合并每个交易的解找到整个网络的最优解, 会产生较大的解空间。2) 路径状态不可预测。发送者只能跟踪已连接通道的瞬时状态, 而不能跟踪整个路径状态。PCN 可以提供强大的隐私保护, 使发送者在其交易路径上无法获得有关其他并发交易的信息。此外, 动态并发交易会导致中间用户和信道链路上的交易数据包数量快速变化, 使路径状态不可预测。3) 链路容量竞争。在共享节点上, 并发交易争夺转发容量。由于每个节点的容量是固定的, 因此当为其他交易分配较高优先级时, 低优先级交易的转发率会下降。为了抵消优先级调整的影响, 发送方需要提高交易优先级, 与其他渠道竞争通道容量。

本文主要的创新点如下。

1) 构建了交易路径确定背景下 PCN 中同向和双向交易调度模型, 引入交易优先级, 同时考虑交易时间对 PCN 优化的影响。基于此, 建立了一个多目标优化问题, 将其分解并转化为交易优先级优化和交易转发顺序优化 2 个子问题, 以实现最大化交易成功率和最小化交易起始金额。

2) 提出了一种基于截止时间的优先级博弈调度 (PGSD, priority game scheduling based on deadline) 算法, 将所构建的 2 个子问题转化成 2 个相互关联的博弈, 采用合作博弈对优化目标进行求解, 通过重复博弈和策略更新找到最优策略以达到动态纳什均衡, 最终实现 PCN 中交易的有效调度。

3) 利用基于闪电网络的子网和瓦茨-斯特罗加茨小世界模型实现 PCN 仿真, 并基于 Kaggle 信用卡

数据集实现实验仿真,以验证本文所提调度算法的有效性。与其他 3 种基准算法相比,本文算法能实现更高的交易成功率和更低的交易初始金额。

### 1 系统模型

本文构建的 PCN 双向交易系统架构如图 1 所示,目标是优化 PCN 的长期交易,降低链下支付通道频繁开闭导致的资源消耗。

PCN 可以看作一个直接图  $G=(\mathcal{V},\mathcal{E})$ ,其中  $\mathcal{V}$  是 PCN 所有节点的集合,  $\mathcal{V}=\{1,\dots,v,\dots,V\}$ ,  $V$  表示所有节点的个数,  $\mathcal{E}$  是 PCN 所有通道的集合,  $\mathcal{E}=\{e_{ij}\},i,j\in\mathcal{V}$ 。每个节点至少有一个通道连接到其他节点,其既可以作为起点发起交易,也可以作为终点接收交易,还可以作为中继节点转发交易。PCN 的支付通道可以是单向的也可以是双向的,本文主要讨论双向支付通道情况下 PCN 的交易调度。假设在时间段  $T$  内,共有  $N$  个交易在 PCN 生成。每个交易的特征是起点、终点、交易时间戳(交易生成时间)、金额、交易路由和交易截止日期,即  $\mathbb{T}_x=\{u,v,\tau_x^s,d_x,p_x,\tau_x^d\},x\in\mathcal{N},\mathcal{N}=\{1,\dots,x,\dots,N\}$ 。其中,交易  $\mathbb{T}_x$  使用预先指定的路径  $p_x$  完成交易,起点为  $u$ ,终点为  $v$ ,并且  $u,v\in\mathcal{V}$ 。 $p_x$  路由路径可以由

中继节点序列  $p_x=\{u,\dots,i,\dots,v\}$  表示。定义一个数组表示交易  $\mathbb{T}_x$  到达中继节点  $i$  且在路径  $p_x$  上剩余的中继节点序列  $r_x=\{i,j,\dots,v\},j\in r_x\in p_x$ ,  $j$  是路径  $p_x$  中的另一个中继节点。中继节点  $i$  转发交易  $\mathbb{T}_x$  到下一跳节点需要提供的转发费用为  $f_i^x$ ,每经过一个中继节点都需要支付一定的转发费用。不同的转发费用往往会影响到交易时间,从而影响到交易成功率。在每个节点处设计一个缓冲区,假设每个缓冲区的通道容量是不受限制的。定义交易的金额为  $d_x$ ,交易生成时间为  $\tau_x^s$ ,交易完成截止日期为  $\tau_x^d$ ,交易通过的路径已知,需通过  $h_x\in\{1,2,\dots\}$  跳,其中通过通道的时间忽略不计。

#### 1.1 交易截止日期

当支付通道打开时,终点首先生成一个随机值  $Q$ ,并将其哈希值  $R$  发送给起点。起点以及任何中间用户都将哈希值  $R$  包含在交易合同中,这样只有当哈希值  $R$  被提供给终点时,终点才能领到交易的款项,随后起点交易完成。然而,每个交易都受到哈希时间锁合约 (HTLC, Hash time lock contract) 容忍度的限制  $\tau_x^d$ ,即交易截止时间。如果中继节点或终点在 HTLC 容忍度内没有收到哈希值  $R$ ,那么转让的费用将被退还给起点。HTLC 容忍度的单位

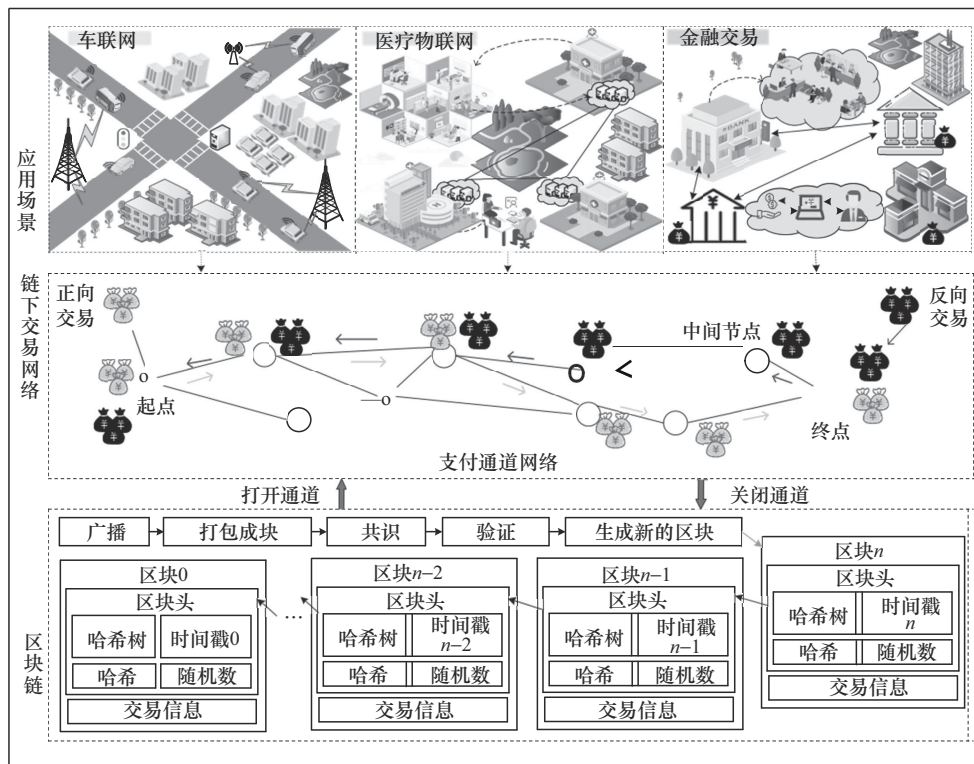


图 1 PCN 双向交易系统架构

用  $\delta$  表示, 定义为完成一个单跳交易最坏情况下的时间约束。支付路径中的每个用户都设置了一个容忍度, 且出支付通道的 HTLC 容忍度比入支付通道的 HTLC 容忍度小。HTLC 能够使用时间锁创建  $\tau_x^d$  内完成的交易, 当超过该时间时, 此交易将失败。交易实际完成所花费的时间应该小于交易要求的截止时间, 即  $\tau_x^w + \tau_x^s \leq \tau_x^d$ , 其中,  $\tau_x^w$  表示完成交易  $\mathbb{T}_x$  的实际时间。

### 1.2 交易顺序

交易在每个共享的中继节点上争夺转发能力, 转发的交易顺序不同, 交易成功率不同。

#### 1.2.1 同向交易顺序

每条通道  $e_{ij}$  均有通道平衡  $b_{ij}(t)$ , 表示在  $t$  时刻节点  $i$  到节点  $j$  最大限度可以转移的费用。其中,  $t \in \{0, 1, \dots, T\}$ 。同样  $b_{ji}(t)$  表示在  $t$  时刻从节点  $j$  到节点  $i$  最大限度可以转移的费用。对于通道  $e_{ij} \in \mathcal{E}$ , 使用  $C_{ij}$  表示该通道的金额,  $C_{ij} = b_{ij}(t) + b_{ji}(t)$ 。根据 HTLC 协议, 一条支付通道的总金额是固定的, 它包括 2 个节点在这条通道的金额。随着交易的发生, 这 2 个节点的金额可能会相互转移, 但是它们的总金额是不发生变化的, 即  $C_{ij}$  不随时间变化。对于交易  $\mathbb{T}_x$ , 起始节点  $u$  的起始金额  $b_{u,i}(t_0)$  和中继节点  $i$  限制了交易成功率, 起始节点的金额需要大于或等于该交易的实际支付金额与该交易在所有中继节点的转发总金额之和, 其中  $t_0$  表示  $t = 0$  时刻。对于节点  $i$  来说, 在时间段  $T$  内, 节点  $i$  的初始金额需要满足经过该节点的所有交易的实际支付金额和交易的剩余节点的转发费用之和。

在节点处设置了  $K$  个优先级, 其中  $\mathcal{K} = \{1, \dots, k, \dots, K\}$ , 每个交易到达每个节点都会分配一个优先级, 且每个交易在其路径上的不同节点分配的优先级不同, 交易的优先级数字越小, 则该交易越优先转发。如图 2 所示, 交易  $\mathbb{T}_1$  的优先级为 1, 而交易  $\mathbb{T}_2$  的优先级为 2, 当交易  $\mathbb{T}_1$  和  $\mathbb{T}_2$  同时到达中继节点  $i$  时, 交易  $\mathbb{T}_1$  优先转发。

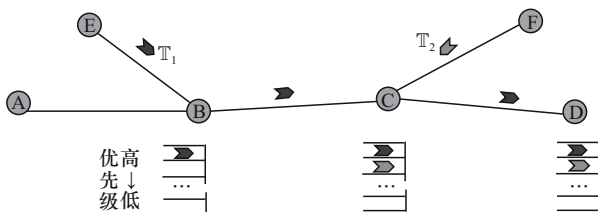


图 2 同向交易转发

定义  $F_x^i$  表示路径为  $p_x$  的交易经过中继节点  $i$  到终点  $v$  上需要支付的实际转发费用, 如式(1)所示。

$$F_x^i = \sum_{i \in r_x} f_i^x = \sum_{i \in r_x} \sum_{k=1}^K \chi_i^{x,k} c_i^k \quad (1)$$

其中,  $f_i^x$  是交易  $\mathbb{T}_x$  在中继节点  $i$  的转发费用,  $c_i^k$  是已知在中继节点  $i$  优先级为  $k$  的交易对应的转发费用,  $\chi_i^{x,k}$  是优先级分配单元的二进制变量, 如果路径为  $p_x$  的交易  $\mathbb{T}_x$  在中继节点  $i$  被分配优先级  $k$ , 则  $\chi_i^{x,k} = 1$ , 否则  $\chi_i^{x,k} = 0$ 。每个中继节点对应的优先级是唯一确定的, 即

$$\sum_{k=1}^K \chi_i^{x,k} = 1 \quad (2)$$

由于每个中继节点交易到达的动态性, 本文无法提前了解其他交易是否到达, 以及每个交易的优先级, 因此同一个交易在不同中继节点的优先级是不同的, 那么相应的转发顺序也是不同的。但在同一个中继节点处, 每个交易的优先级和具体的转发顺序相对一致, 优先级越高即  $k$  值越小, 则转发顺序越优先。交易需要在中继节点处争夺转发能力。不同的转发顺序对交易的吞吐量和初始金额具有不同的影响。为了能够通过多个中继节点到最终目的地的通道网络来构建安全传输, 需要 HTLC 参与。HTLC 能够使用时间锁创建某些只在某个时间内完成的交易, 这与  $\tau_x^d - \tau_x^s$  和交易顺序相关。可以通过增加优先级实现立即转发, 但同时会增加交易转发费用, 从而导致初始金额增加。发送者可以保持较低的优先级以节约交易的转发费用, 实现较低的初始金额, 从而不影响区块链上的交易。

#### 1.2.2 双向交易顺序

通道的剩余金额和交易截止时间可以用来决策交易的正反方向。双向交易顺序的存在, 对通道余额具有一定的影响。相对来说, 频繁的双向交易有利于初始金额的最小化。但是频繁的双向交易会增加交易时间, 甚至可能超出交易的截止时间, 从而导致交易失败。假设在  $t$  时刻, 同一个支付通道  $e_{ij}$  只能正向或者反向转发一个交易, 如图 3 所示。用  $\zeta_i(t)$  表示中继节点  $i$  在  $t$  时刻的交易转发方向,  $\zeta_i(t) \in \{-1, 0, 1\}$ 。其中,  $\zeta_i(t) = 0$  表示不转发交易或者没有转发交易,  $\zeta_i(t) = 1$  表示正向转发交易,  $\zeta_i(t) = -1$  表示反向转发交易。考虑通道双向交易的截止日期和通道两端节点的剩余金额对交易的方

向进行调度,交易的截止时间需要大于交易生成时间与实际完成时间之和。

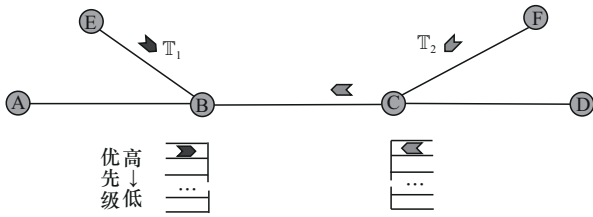


图3 双向交易转发

PCN的交易量与每个交易是否成功有关。定义 $\lambda$ 为单位时间内支付通道网络的交易成功率,表示为

$$\lambda = \frac{S}{N} = \frac{\sum_{t=0}^T \sum_{i \in p_x} \prod_{i \in p_x} a_x^i(t)}{NT} \quad (3)$$

其中, $N$ 是时间段 $T$ 内交易产生的总数量, $S$ 是时间段 $T$ 内成功完成的交易数量, $a_x^i(t)$ 是交易 $\mathbb{T}_x$ 在 $t$ 时刻中继节点 $i$ 是否交易成功的变量, $\prod_{i \in p_x} a_x^i(t) = 1$ 表示交易 $\mathbb{T}_x$ 在截止时间内交易成功, $\prod_{i \in p_x} a_x^i(t) = 0$ 表示交易 $\mathbb{T}_x$ 在截止时间内交易失败。 $\sum_{x=1}^N \prod_{i \in p_x} a_x^i(t)$ 表示在时间段 $T$ 内成功完成的交易数量。

在 $T$ 时间段内,交易 $\mathbb{T}_x$ 需要经过 $h_x$ 个中继节点。这需要在每个中继节点判断交易完成的情况。在中继节点处的交易成功与否不仅与中继节点 $i$ 有关,还与具体交易的时间有关。当交易 $\mathbb{T}_x$ 在中继节点 $i$ 满足交易的截止时间大于或等于实际交易时间和交易生成时间之和时,即 $\tau_x^d \geq \tau_x^i + \tau_x^{iv}$ ,则交易 $\mathbb{T}_x$ 交易成功,否则交易失败。其中, $\tau_x^i$ 是交易 $\mathbb{T}_x$ 到达中继节点 $i$ 的时间, $\tau_x^{iv}$ 是交易 $\mathbb{T}_x$ 从中继节点 $i$ 到达终点 $v$ 的实际时间。

当 $t$ 时刻交易 $\mathbb{T}_x$ 在中继节点 $i$ 处并准备转发到下一跳节点时,若满足该中继节点的金额大于或等于实际交易费用和剩余中继节点转发费用之和,即 $b_{ij}(t) \geq d_x + F_x^i$ ,则交易 $\mathbb{T}_x$ 交易成功,否则交易失败。只有当交易 $\mathbb{T}_x$ 同时满足时间和费用这2个条件时,才能保证交易 $\mathbb{T}_x$ 在中继节点 $i$ 处转发成功,即 $a_x^i(t) = 1$ ;仅满足其中一个条件或者都不满足的情况下,交易失败,即 $a_x^i(t) = 0$ 。当交易截止时间 $\tau_x^d$ 大于或等于交易到达节点 $i$ 的时间 $\tau_x^i$ 和交易完成时间之和,并且当前该节点的通道余额 $b_{ij}(t)$ 大于或

等于剩余中继节点转发费用 $F_x^i$ 和交易金额 $d_x$ 之和时,中继节点 $i$ 交易成功,即 $a_x^i(t) = 1$ ;在其他情况下,中继节点 $i$ 交易失败,即 $a_x^i(t) = 0$ 。

### 1.2.3 初始金额优化

初始金额需要考虑到双向交易的转发顺序和转发费用,影响节点初始金额的因素包含同向交易顺序和反向交易顺序。当发生正向交易时,节点需要支付交易的实际金额和中继转发费用;当发生反向交易时,节点则会收到反向交易的实际金额和中继转发费用。

1) 当节点为起始节点时,正向交易成功完成后,节点需要支付的金额为实际交易金额与所有经过的中继节点的转发费用之和。

2) 当节点为中继节点时,正向(反向)交易成功完成后,节点支付(收到)的金额为实际交易金额与经过该节点后剩余的中继节点的转发费用之和。

3) 当节点为终点时,反向交易成功完成后,节点收到的金额为实际交易的金额。

当然每个节点都可能在某个时刻为起始节点,而在另一个时刻为中继节点。而且节点 $i$ 在时间段 $T$ 内可能不仅仅转发(或发起)一个交易,这需要符合要求的交易进行综合考虑,可以优化在时间段 $T$ 内节点 $i$ 的初始金额。

$$\max \left\{ 0, \sum_{t=0}^T \sum_{i=1}^N \zeta_i(t) \phi_x^{ij}(t) \left( \prod_{i \in p_x} a_x^i(t) \right) (d_x + F_x^i) \right\} \leq b_{ij}(t_0), i, j \in p_x \quad (4)$$

其中, $\phi_x^{ij}(t)$ 是一个判断交易 $\mathbb{T}_x$ 是否在 $t$ 时刻通过通道 $e_{ij}$ 或 $e_{ji}$ 的二进制辅助变量,当交易 $\mathbb{T}_x$ 通过通道 $e_{ij}$ 或 $e_{ji}$ 时, $\phi_x^{ij}(t) = 1$ ,否则 $\phi_x^{ij}(t) = 0$ ;  $b_{ij}(t_0)$ 为节点 $i$ 在时间段 $T$ 内通道 $e_{ij}$ 的初始金额。

随时间变化,节点 $i$ 在通道 $e_{ij}$ 中的金额 $b_{ij}(t)$ 是不断变化的,但是整个通道的总金额是固定不变的,即 $C_{ij}$ 不随时间变化。在 $t$ 时刻,经过节点 $ij$ 交易的最大花费不能超过该通道的金额 $C_{ij}$ ,即

$$d_x + \phi_x^{ij}(t) a_x^i(t) F_x^i \leq C_{ij} \quad (5)$$

## 2 解决方案

### 2.1 问题描述

当交易 $\mathbb{T}_x$ 到达中继节点 $i$ 时,需要通过其交易

优先级和通道剩余余额判断交易方向和交易顺序，目标是最大化交易成功率和最小化初始金额。

$$\begin{aligned}
 \text{P1: } & \max_{\zeta_i(t), \chi_i^{x,k}} \lambda \\
 & \min_{\zeta_i(t), \chi_i^{x,k}} b_{ij}(t_0) \\
 \text{s.t. } & \text{C1: } d_x + \phi_x^{ij}(t) a_x^i(t) F_x^i \leq C_{ij}, \\
 & \quad \forall e_{ij} \in \mathcal{E}, i \in \mathcal{V}, x \in \mathcal{N} \\
 & \text{C2: } \sum_{t=0}^T \sum_{x=1}^N \zeta_i(t) \phi_x^{ij}(t) \left( \prod_{i \in p_x} a_x^i(t) \right) (d_x + F_x^i) \leq \\
 & \quad b_{ij}(t_0), \forall ij \in p_x, e_{ij} \in \mathcal{E} \\
 & \text{C3: } \sum_{k=1}^K \chi_i^{x,k} = 1, \forall i \in \mathcal{V}, x \in \mathcal{N} \\
 & \text{C4: } \zeta_i(t) \in \{-1, 0, 1\}, \forall i \in \mathcal{V} \\
 & \text{C5: } \tau_x^w + \tau_x^s \leq \tau_x^d, x \in \mathcal{N} \quad (6)
 \end{aligned}$$

其中，约束 C1 表示每个交易的最大花费金额（包括实际支付金额和转发费用）的限制；约束 C2 表示每个节点初始金额的范围；约束 C3 表示每个交易  $\mathbb{T}_x$  只存在一个优先级；约束 C4 表示在中继节点  $i$  的交易方向变量；约束 C5 表示每个交易的时间约束。由于交易优先级与交易转发方向的动态耦合性，以及多个约束条件的复杂性，问题 P1 属于典型的 NP 难问题。

**定理 1** 节点在  $T$  个时间段的初始金额等价于节点在这  $T$  个时间段内的净支出。

**证明** 节点在  $T$  个时间段中的净支出等于节点在  $T$  个时间段中转发所有交易花费的费用和接收所有交易得到的费用之和。由于优化目标之一是在  $T$  个时间段中的 PCN 节点的初始金额，可以将节点在  $T$  个时间段的初始金额等价于节点在这  $T$  个时间段的净支出。它们在物理意义上是相同的，即最小化节点的初始金额为最小化  $T$  个时间段的净支出。证毕。

通过定理 1，对问题 P1 中的第二个优化问题进行转化，等价于最小化在  $T$  时间段中的节点净支出  $g_{ij}^x(t)$ （花费的金额和收入的金额的加权和），即

$$\begin{aligned}
 \min g_{ij}^x(t) &= \sum_{t=0}^T \sum_{x=1}^N \zeta_i(t) \phi_x^{ij}(t) \left( \prod_{i \in p_x} a_x^i(t) \right) (d_x + F_x^i) \\
 & \quad ij \in p_x, e_{ij} \in \mathcal{E} \\
 \text{s.t. } & g_{ij}^x(t) \geq 0 \quad (7)
 \end{aligned}$$

为了简化问题求解，问题 P1 优化目标可转化为

$$\begin{aligned}
 \text{P2: } & \max_{\zeta_i(t), \chi_i^{x,k}} \sum_{x=1}^N \prod_{i \in p_x} a_x^i(t) \\
 & \min_{\zeta_i(t), \chi_i^{x,k}} g_{ij}^x(t) \\
 \text{s.t. } & \text{C1: } d_x + \phi_x^{ij}(t) a_x^i(t) F_x^i \leq C_{ij}, \\
 & \quad \forall e_{ij} \in \mathcal{E}, i \in \mathcal{V}, x \in \mathcal{N} \\
 & \text{C2: } g_{ij}^x(t) \geq 0 \\
 & \text{C3: } \sum_{k=1}^K \chi_i^{x,k} = 1, \forall i \in \mathcal{V}, x \in \mathcal{N} \\
 & \text{C4: } \zeta_i(t) \in \{-1, 0, 1\}, \forall i \in \mathcal{V} \\
 & \text{C5: } \tau_x^w + \tau_x^s \leq \tau_x^d, x \in \mathcal{N} \quad (8)
 \end{aligned}$$

其中，约束 C1 和 C3~C5 由问题 P1 中的 C1 和 C3~C5 得来；约束 C2 由问题 P1 中的 C2 松弛得来，由定理 1 可获得。

由于问题 P2 中的 2 个优化变量高度耦合，上述多目标优化问题无法直接分解。为了方便求解多目标优化问题，本文将  $\frac{g_{ij}^x(t)}{\sum_{x=1}^N \prod_{i \in p_x} a_x^i(t)}$  定义为成功完成的交易在节点  $i$  的平均净支出费用，那么问题 P2 可转化为

$$\begin{aligned}
 \text{P3: } & \min_{\zeta_i(t), \chi_i^{x,k}} \frac{g_{ij}^x(t)}{\sum_{x=1}^N \prod_{i \in p_x} a_x^i(t)} \\
 \text{s.t. } & \text{C1: } d_x + \phi_x^{ij}(t) a_x^i(t) \left( \sum_{i \in r_x} \sum_{k=1}^K \chi_i^{x,k} c_i^k \right) \leq \\
 & \quad C_{ij}, \forall e_{ij} \in \mathcal{E}, i \in \mathcal{V}, x \in \mathcal{N} \\
 & \text{C2: } g_{ij}^x(t) \geq 0 \\
 & \text{C3: } \sum_{k=1}^K \chi_i^{x,k} = 1, \forall i \in \mathcal{V}, x \in \mathcal{N} \\
 & \text{C4: } \zeta_i(t) \in \{-1, 0, 1\}, \forall i \in \mathcal{V} \\
 & \text{C5: } \tau_x^w + \tau_x^s \leq \tau_x^d, x \in \mathcal{N} \quad (9)
 \end{aligned}$$

其中，约束 C1~C5 是问题 P2 中的 C1~C5。

在  $T$  时间段内，每个交易  $\mathbb{T}_x$  需要经过  $h_x$  个中继节点。为了提高交易的速率，需要在每个中继节点判断交易完成的情况。在中继节点处的交易成功与否不仅与中继节点  $i$  有关，还与具体交易的时间有关。

$$a_x^i(t) = \alpha_x^i \beta_x^i(t) \quad (10)$$

其中， $\alpha_x^i$  为在中继节点  $i$  判断交易  $\mathbb{T}_x$  的实际交易时间是否满足交易截止时间的二进制变量，当交易  $\mathbb{T}_x$  在中继节点  $i$  时满足交易截止时间大于或等于实际交易时间和交易生成时间  $\tau_x^d \geq \tau_x^i + \tau_x^{iv}$ ，则

$\alpha_x^i = 1$ , 反之  $\alpha_x^i = 0$ ;  $\beta_x^i(t)$  为判断中继节点是否满足交易  $\mathbb{T}_x$  的交易费用 (包括实际交易费用和之后中继节点的转发费用) 的二进制变量, 当  $t$  时刻交易  $\mathbb{T}_x$  在中继节点  $i$  准备转发到下一跳节点时, 满足该中继节点的金额大于或等于实际交易费用和剩余中继节点转发费用之和, 即  $b_{ij}(t) \geq d_x + F_x^i$ , 则  $\beta_x^i(t) = 1$ , 交易  $\mathbb{T}_x$  成功, 否则  $\beta_x^i(t) = 0$ , 交易  $\mathbb{T}_x$  失败。当交易  $\mathbb{T}_x$  同时满足时间和费用 2 个条件时, 即  $\alpha_x^i = 1$  且  $\beta_x^i(t) = 1$ , 才能保证交易  $\mathbb{T}_x$  在中继节点  $i$  处转发成功, 即  $a_x^i(t) = 1$ ; 只满足其中一个条件或者都不满足的情况下交易失败, 即  $a_x^i(t) = 0$ 。

由于无法直接得出从中继节点  $i$  到终点  $v$  的交易完成时间  $\tau_x^{iv}$ , 因此在交易经过每个中继节点  $i$  时对其交易完成时间进行预估。将优先级为  $k$  的交易  $\mathbb{T}_x$  在路径  $p_x$  从中继节点  $i$  到终点  $v$  的最大预估完成时间定义为  $\mathcal{T}_x^{iv}$ , 即多个中继节点交易完成的最大预估时间之和。

$$\mathcal{T}_x^{iv} = \sum_{i \in r_x} \mathcal{T}_x^{ij} \quad j \in r_x \quad (11)$$

其中,  $\mathcal{T}_x^{ij}$  是交易  $\mathbb{T}_x$  在中继节点  $i$  到下一个中继节点的最大预估交易完成时间。

每个交易在一个中继节点的交易花费时间包括当前中继节点的缓存区等待时间、交易从一个中继节点转发到下一个中继节点的交易时间。每个中继节点的缓存区存在 2 种情况: 1) 当  $t$  时刻交易  $\mathbb{T}_x$  到达中继节点  $i$  时, 中继节点  $i$  的交易方向与到达的交易  $\mathbb{T}_x$  的方向相同, 则交易  $\mathbb{T}_x$  在中继节点  $i$  的等待时间为优先级高于该交易的其他交易时间之和; 2) 当  $t$  时刻交易  $\mathbb{T}_x$  到达中继节点  $i$  时, 中继节点  $i$  的交易方向与到达的交易  $\mathbb{T}_x$  的方向相反, 则交易  $\mathbb{T}_x$  在中继节点  $i$  的交易等待时间为两部分等待时间之和, 即节点等待交易方向发生变化的时间与优先级高于该交易的其他交易时间之和。

定义  $\zeta_x$  为交易  $\mathbb{T}_x$  的交易方向,  $\zeta_x = 1$  表示交易  $\mathbb{T}_x$  的交易方向为正向,  $\zeta_x = -1$  表示交易  $\mathbb{T}_x$  的交易方向为反向。交易  $\mathbb{T}_x$  从中继节点  $i$  到下一个中继节点的最大预估交易完成时间为

$$\mathcal{T}_x^{ij} = \begin{cases} \sum_{\substack{x'=1 \\ x' \neq x}}^N \sum_{k=1}^{k-1} \mathcal{T}_x^{ij} \chi_i^{x',k'} + \mathcal{T}^{ij}, a = 1 \\ \sum_{\substack{x'=1 \\ x' \neq x}}^N \sum_{k=1}^{k-1} \mathcal{T}_x^{ij} \chi_i^{x',k'} + \Delta_x^{ij}(t+1) + \mathcal{T}^{ij}, a = -1 \end{cases} \quad (12)$$

s.t.  $a = \zeta_x \zeta_i(t), k-1 \in \mathcal{K}, i, j \in r_x$

其中,  $\mathcal{T}^{ij}$  表示优先转发的交易在路径  $p_x$  上通过一个支付通道  $e_{ij}$  的最大预估交易时间,  $\sum_{\substack{x'=1 \\ x' \neq x}}^N \sum_{k=1}^{k-1} \mathcal{T}_x^{ij} \chi_i^{x',k'}$  表示在中继节点  $i$  交易  $\mathbb{T}_x$  存在的队列中优先级高于交易  $\mathbb{T}_x$  的预估交易时间之和,  $\Delta_x^{ij}(t)$  表示交易  $\mathbb{T}_x$  在中继节点  $i$  等待的反向交易时间。

关联变量  $\ell_x^{ij}(t)$  表示节点  $i$  转发方向和交易  $\mathbb{T}_x$  方向的关系,  $\ell_x^{ij}(t) = 1$  表示节点  $i$  转发方向和交易  $\mathbb{T}_x$  方向是反向,  $\ell_x^{ij}(t) = 0$  表示节点转发方向和交易方向是同向。由式(12)可得出交易  $\mathbb{T}_x$  在中继节点  $i$  到下一个中继节点的最大预估交易完成时间为

$$\mathcal{T}_x^{ij} = \sum_{\substack{x'=1 \\ x' \neq x}}^N \sum_{k=1}^{k-1} \mathcal{T}_x^{ij} \chi_i^{x',k'} + \ell_x^{ij}(t) \Delta_x^{ij}(t+1) + \mathcal{T}^{ij}, \quad k-1 \in \mathcal{K}, i, j \in r_x \quad (13)$$

其中,  $\chi_i^{x',k'}$  是交易  $\mathbb{T}_x$  在节点  $i$  的二进制优先级分配,  $\ell_x^{ij}(t)$  是节点转发方向和交易方向的关系辅助变量,  $\Delta_x^{ij}(t+1)$  是交易  $\mathbb{T}_x$  在节点  $i$  等待的反向交易时间,  $\mathcal{T}^{ij}$  是优先转发的交易在路径  $p_x$  上的一个支付通道  $e_{ij}$  的最大交易时间。

**定理 2** 当前时刻  $t$  与上一时刻  $t-1$  的交易方向相反, 即  $\zeta_i(t) + \zeta_i(t-1) = 0$  时 (如交易方向是正向, 而上一时刻交易方向为反向, 那么当前时刻为正向), 交易  $\mathbb{T}_x$  等待的反向交易时间为  $\mathcal{T}^{ij}$ 。

**证明** 当该反向交易没有完成时, 一个支付通道  $e_{ij}$  两端的节点金额不发生相应的变化。除了正在交易的反向交易外, 其余在各自队列中的交易等待时间也相应增加。所以中继节点  $i$  在  $\mathcal{T}^{ij}$  时间段内的任何时刻转发方向不会发生变化, 直至该反向交易完成。除  $\zeta_i(t) + \zeta_i(t-1) = 0$  情况外, 那么就是上一时刻  $t-1$  和当前时刻  $t$  节点  $i$  转发方向相同, 则需要考虑下一时刻  $t+1$  节点  $i$  是否发生转发方向变化。重复上述循环, 直至转发方向发生变化, 累加等待的反向交易时间。证毕。

基于定理 2, 可以得出交易  $\mathbb{T}_x$  在中继节点  $i$  等待的反向交易时间  $\Delta_x^{ij}(t)$  为

$$\Delta_x^{ij}(t) = \begin{cases} \mathcal{T}^{ij}, \zeta_i(t) + \zeta_i(t-1) = 0 \\ \mathcal{T}^{ij} + \Delta_x^{ij}(t+1), \text{其他} \end{cases}, i, j \in r_x \quad (14)$$

其中,  $\mathcal{T}^{ij}$  是最优先转发的交易在路径上的一个支

付通道  $e_{ij}$  的最大交易时间。

为了更好地预估交易完成一个支付通道需要的最大时间  $\mathcal{T}^{ij}$ ，本文利用文献[19]中的方法，对同一路径交易平均时间进行求解。假设交易  $\mathbb{T}_y$  和交易  $\mathbb{T}_x$  是同一路径的交易，即  $p_x = p_y$ ，且在交易  $\mathbb{T}_y$  之后，在此路径上还没有其他完成的交易。然后可以预测交易  $\mathbb{T}_x$  在路径  $p_x$  上完成交易所需的平均时间，并用  $\bar{\tau}_x$  表示。基于交易的平均完成时间  $\bar{\tau}_y$  和交易已完成的时间  $\tau_y^w$ ，更新  $\bar{\tau}_x$  的值，即对  $\tau_y^w$  样本设置权重。

$$\bar{\tau}_x = (1 - \gamma)\bar{\tau}_y + \gamma\tau_y^w \quad (15)$$

其中， $0 \leq \gamma \leq 1$ ， $\gamma$  是常数。基于此预估交易  $\mathbb{T}_x$  在路径  $p_x$  上的一个支付通道  $e_{ij}$  的平均交易时间为

$$\bar{\tau}_x^{ij} = \frac{\bar{\tau}_x}{h_x} \quad (16)$$

由于考虑预估平均交易时间，而且在 PCN 中的中继节点转发的交易是动态的，无法衡量具有不同优先级的交易在一个支付通道  $e_{ij}$  的预估平均交易时间，因此本文给出定义 1。

**定义 1** 将交易  $\mathbb{T}_x$ （优先级为 1 的交易  $\mathbb{T}_x$ ）在路径  $p_x$  上的一个支付通道  $e_{ij}$  的最大预估交易时间定义为  $\mathcal{T}^{ij}$ ，且  $\mathcal{T}^{ij} = \bar{\tau}_x^{ij}$ 。

当在一个支付通道的平均交易时间是  $\bar{\tau}_x^{ij}$  的交易  $\mathbb{T}_x$  具有最低优先级（即优先级为 1）时，那么可以认为  $\bar{\tau}_x^{ij}$  在数值上等同于一个具有最低优先级（即优先级为 1）交易在一个支付通道  $e_{ij}$  的最大预估交易时间  $\mathcal{T}^{ij}$ ，即  $\mathcal{T}^{ij} = \bar{\tau}_x^{ij}$ 。只有当具有最低优先级交易  $\mathbb{T}_x$  的一个支付通道  $e_{ij}$  预估交易时间  $\mathcal{T}^{ij}$  等于该平均交易时间  $\bar{\tau}_x^{ij}$  时，交易  $\mathbb{T}_x$  在一个支付通道  $e_{ij}$  预估交易时间  $\mathcal{T}_x^{ij}$  的数值最大。在此基础上，对交易在路径上的最大交易时间进行预估，只要预估的最大交易时间满足交易截止时间，那么存在该交易的实际交易时间将会满足交易截止时间的约束。

## 2.2 优先级分配

优化每个交易在每个中继节点的优先级，即交易多节点优先级分配。在确定交易路径上的节点在每个时刻的交易转发方向前提下，分配每个交易在路径上的优先级。此时，从当前中继节点到下一个中继节点的最大预估交易完成时间只与交易优先级相关。当确定交易与节点交易方向的关系时，每个

成功的交易在节点的净支出费用只与交易的优先级相关。

在每个中继节点  $i$  处对交易  $\mathbb{T}_x$  的最大完成时间进行预测，若满足交易截止时间  $\tau_x^d$  大于或等于到达中继节点  $i$  的时间  $\tau_x^i$  和最大预估交易时间  $\mathcal{T}_x^{i,v}$ ，即

$$\tau_x^d - \tau_x^i \geq \mathcal{T}_x^{i,v} \quad (17)$$

则继续在队列中等待交易转发，其中

$$\mathcal{T}_x^{i,v} = \sum_{i \in r_x} \mathcal{T}_x^{ij} = \sum_{i \in r_x} \left( \sum_{\substack{x'=1 \\ x' \neq x}}^N \sum_{k'=1}^{k-1} \mathcal{T}_{x'}^{ij} \chi_i^{x',k'} + \ell_x^{ij}(t) \Delta_x^{ij}(t+1) + \mathcal{T}^{ij} \right) \quad (18)$$

因此， $\alpha_x^i$  满足

$$\alpha_x^i = \begin{cases} 1, & \tau_x^d - \sum_{i \in r_x} \left( \sum_{\substack{x'=1 \\ x' \neq x}}^N \sum_{k'=1}^{k-1} \mathcal{T}_{x'}^{ij} \chi_i^{x',k'} + z \right) \geq \tau_x^i \\ 0, & \text{其他} \end{cases} \quad (19)$$

当固定节点转发方向时，节点转发方向和交易方向的关系也是固定的，即  $\ell_x^{ij}(t)$  是已知的， $z$  为一个常数，且  $z = \ell_x^{ij}(t) \Delta_x^{ij}(t+1) + \mathcal{T}^{ij}$ 。

第一个子问题可通过对交易在每个节点的优先级分配来最小化成功交易在节点的净支出费用，问题可构建为

$$\begin{aligned} \text{P4: } & \min \frac{g_{ij}^x(t)}{\sum_{x=1}^N \prod_{i \in p_x} (\tilde{\alpha}_x^i \tilde{\beta}_x^i(t))} \\ \text{s.t. } & \text{C1: } d_x + \phi_x^{ij}(t) (\tilde{\alpha}_x^i \tilde{\beta}_x^i(t)) \left( \sum_{i \in r_x} \sum_{k=1}^K \chi_i^{x,k} c_i^k \right) \leq C_{ij}, \\ & \forall e_{ij} \in \mathcal{E}, i \in \mathcal{V}, x \in \mathcal{N} \\ & \text{C2: } g_{ij}^x(t) \geq 0 \\ & \text{C3: } \sum_{k=1}^K \chi_i^{x,k} = 1, \forall i \in \mathcal{V}, x \in \mathcal{N} \\ & \text{C4: } \sum_{i \in p_x} \left( \sum_{\substack{x'=1 \\ x' \neq x}}^N \sum_{k'=1}^{k-1} \mathcal{T}_{x'}^{ij} \chi_i^{x',k'} + z \right) \leq \tau_x^d - \tau_x^s, x \in \mathcal{N} \end{aligned} \quad (20)$$

其中，约束 C1 由问题 P3 中的 C1 松弛得来；约束 C2~C3 是问题 P3 中的 C2~C3；约束 C4 由问题 P3 中

的C5松弛得来。

$$\tilde{\alpha}_x^i = \begin{cases} 1, \tau_x^d - \sum_{i \in r_x} \left( \sum_{\substack{x'=1 \\ x' \neq x}}^{k-1} \sum_{k'=1}^N \mathcal{T}_x^{ij} \chi_i^{x',k'} + z \right) \geq \tau_x^i \\ 0, \text{其他} \end{cases}$$

$$\tilde{\beta}_x^i(t) = \begin{cases} 1, b_{ij}(t) - d_x \geq \sum_{i \in r_x, k=1}^K \chi_i^{x,k} c_i^k \\ 0, \text{其他} \end{cases}$$

### 2.3 节点转发方向决策

子问题2是在固定交易优先级的条件下, 通过优化交易经过的节点的交易转发方向实现最小化成功交易在节点的净支出, 即

$$\text{P5: } \min_{\zeta_i(t)} \frac{g_{ij}^x(t)}{\sum_{i \in p_x} \prod (\alpha_x^i \beta_x^i(t))}$$

$$\text{s.t. C1: } d_x + \phi_x^{ij}(t) (\alpha_x^i \beta_x^i(t)) \left( \sum_{i \in r_x, k=1}^K \chi_i^{x,k} c_i^k \right) \leq C_{ij},$$

$$\forall e_{ij} \in \mathcal{E}, i \in \mathcal{V}, x \in \mathcal{N}$$

$$\text{C2: } g_{ij}^x(t) \geq 0$$

$$\text{C3: } \zeta_i(t) \in \{-1, 0, 1\}, \forall i \in \mathcal{V}$$

$$\text{C4: } \sum_{i \in p_x} \left( \sum_{\substack{x'=1 \\ x' \neq x}}^{k-1} \sum_{k'=1}^N \mathcal{T}_x^{ij} \chi_i^{x',k'} + \mathcal{T}^{ij} + \ell_x^{ij}(t) \Delta_x^{ij}(t+1) \right) \leq \tau_x^d - \tau_x^s, x \in \mathcal{N} \quad (21)$$

其中, 约束C1由问题P3中的C1松弛得来; 约束C2和C3是问题P3中的C2和C4; 约束C4由问题P3中的C5松弛得来。

$$\alpha_x^i = \begin{cases} 1, \tau_x^d - \sum_{i \in r_x} \left( \sum_{\substack{x'=1 \\ x' \neq x}}^{k-1} \sum_{k'=1}^N \mathcal{T}_x^{ij} \chi_i^{x',k'} + \mathcal{T}^{ij} + \ell_x^{ij}(t) \Delta_x^{ij}(t+1) \right) \geq \tau_x^i \\ 0, \text{其他} \end{cases} \quad (22)$$

$$\beta_x^i(t) = \begin{cases} 1, b_{ij}(t) \geq d_x + \sum_{i \in r_x, k=1}^K \chi_i^{x,k} c_i^k \\ 0, \text{其他} \end{cases} \quad (23)$$

### 2.4 博弈求解

本文在文献[20]中的多通道博弈框架上, 将交易优先级和交易转发顺序考虑为2个相互关联的博弈问题。将2个相邻节点作为2个玩家, 第一个

子问题的博弈是这2个玩家合作制定同向交易的优先级, 第二个子问题的博弈是这2个玩家争夺交易优先转发的方向。本文在文献[20]的基础上, 不再局限于玩家的合作, 而是根据子问题的设置, 借助文献[21]提出的网络博弈, 将博弈1和博弈2相结合, 将原来的优化问题转化为多通道网络博弈。

对于博弈 $m$ , 将相关的重复博弈收益定义为玩家每轮平均收益的极限。一个玩家在多通道游戏中的收益被定义为它所有的 $m$ 个重复游戏收益的总和。第一个博弈是相邻节点 $i$ 和 $j$ 作为2个玩家合作决定转发交易在下一个节点 $j$ 的转发优先级。第二个博弈是相邻节点 $i$ 和 $j$ 作为2个玩家竞争当前时刻交易的转发方向。在每个时刻, PCN中2个相邻且存在交易转发的玩家会构成一个玩家队, 同时PCN可能随机出现多个玩家队。本文通过构建一个涵盖2个子问题的博弈模型, 通过双阶段博弈过程进行解析<sup>[22]</sup>。在PCN中, 相应的反应策略表示为

$$\mathbf{Q} = (\mathbf{Q}_{u,l}, \dots, \mathbf{Q}_{i,j}, \dots, \mathbf{Q}_{w,v}) \quad (24)$$

其中,  $\mathbf{Q}_{ij} = (q_{CC}^1, q_{CD}^1, q_{DC}^1, q_{DD}^1; q_{CC}^2, q_{CD}^2, q_{DC}^2, q_{DD}^2)$  是玩家 $i$ 和玩家 $j$ 在博弈中的合作概率, 主要取决于共同玩家 $i$ 和玩家 $j$ 在博弈1和博弈2的先前活动,  $q_{s_i, s_j}^1 \in [0, 1]$ ,  $s_i$ 和 $s_j$ 分别表示玩家 $i$ 和玩家 $j$ 参与的动作。每个玩家会对策略选择进行调整, 以降低其预期成本(成本即负效用)。为了达到优化目标, 在每个博弈中玩家可能采取不同的策略。

博弈1的反应策略可以表示为

$$\mathbf{a}_{s_i, s_j}^1 = \{a_{s_i} a_{s_j}\} \quad (25)$$

其中, 每一个策略对应一个合作率, 通过合作率和效用将进行博弈的动作更新。本文应用反应策略, 基于上一轮合作者的行为来调整当前轮次的反应。定义每个玩家在博弈1中的动作空间为 $\{\chi_i^{x,1}, \dots, \chi_i^{x,k}\}$ , 即 $a_{s_i} \in \{\chi_i^{x,1}, \dots, \chi_i^{x,k}\}$ 和 $a_{s_j} \in \{\chi_i^{x,1}, \dots, \chi_i^{x,k}\}$ 。对于每轮游戏, 反应策略需要指定焦点玩家在下一轮中合作的概率。在式(24)中, 当2个玩家选择同一个优先级时, 相当于2个玩家在博弈1中合作, 其合作概率为 $q_{CC}^1$ 。

博弈2的反应策略可以表示为

$$a_{s_i, s_j}^2 = \begin{pmatrix} (1,1) & (1,0) & (1,-1) \\ (0,1) & (0,0) & (0,-1) \\ (-1,1) & (-1,0) & (-1,-1) \end{pmatrix} \quad (26)$$

然而，在实际 PCN 中，主对角线的反应策略是不可能出现的情况，所以将根据当前通道哪一侧的交易更加紧急，判定 2 个玩家是否合作。基于之前的建模，玩家  $i$  的效用可表示为

$$\mu_i = \mathbb{E}[\mu(\chi_i^{x,k}, \zeta_i(t))] = \mu_i^1 + \mu_i^2 \quad (27)$$

其中， $\mathbb{E}[\cdot]$  表示对其求均值。玩家的目标是在所有的游戏和回合中最大化其收益，通过异步更新实现反应策略的更新。

**定义 2** 纳什均衡。在交易优先级策略配置和节点转发方向策略配置过程中，如果 2 个玩家都选择合作，则构成多通道网络博弈的纯策略纳什均衡。

基于上述模型，求解博弈训练过程如算法 1 所示。

**算法 1** 博弈训练过程

**输入** 两位玩家的反应策略  $q_1$  和  $q_2$ ，支付矩阵  $u$

**输出**  $p, W, A$

- 1)  $m \leftarrow u$  的行数
- 2)  $nA \leftarrow 2^m$
- 3) 初始化  $p$  为长度为 2 的零向量， $c$  为  $m \times 2$  的零矩阵
- 4) 初始化  $A$  为大小为  $nA \times 2$  的零矩阵
- 5) for  $i = 1, 2, \dots, nA$  do
- 6) for  $j = 1, 2, \dots, nA$  do
- 7)  $A[i][j] \leftarrow \text{floor} \frac{i-1}{2^{m-j}} \% 2$
- 8) end for
- 9) end for
- 10) 反转  $A$  的行顺序
- 11) 初始化  $W$  为大小为  $nA^2 \times nA^2$
- 12) for  $i = 1, 2, \dots, nA$  do
- 13) for  $j = 1, 2, \dots, nA$  do
- 14) for  $k = 1, 2, \dots, m$  do
- 15)  $a_1 \leftarrow A[i][k]$
- 16)  $a_2 \leftarrow A[j][k]$
- 17) if  $a_1 = 1$  且  $a_2 = 1$
- 18)  $pA \leftarrow pA + [u[k][1], u[k][1]]$
- 19) elseif  $a_1 = 1$  且  $a_2 = 0$

$$20) \quad pA \leftarrow pA + [u[k][2], u[k][3]]$$

$$21) \quad \text{elseif } a_1 = 0 \text{ 且 } a_2 = 1$$

$$22) \quad pA \leftarrow pA + [u[k][3], u[k][2]]$$

$$23) \quad \text{else}$$

$$24) \quad pA \leftarrow pA + [u[k][4], u[k][4]]$$

$$25) \quad \text{end if}$$

$$26) \quad \text{end for}$$

$$27) \quad \text{end for}$$

$$28) \quad \text{end for}$$

### 3 性能评估

#### 3.1 仿真设置

仿真环境基于 Python 3.8 和 PyCharm2021 软件环境，采用基于闪电网络采样的子网<sup>[23]</sup>，支付通道是根据瓦茨-斯特罗加茨小世界模型<sup>[24]</sup>随机生成的，该模型已被广泛用于描述真实世界的连接。交易路径的长度范围为 4~8，平均长度为 6，与真实的闪电网络相似；每个时间周期为 100 s；根据闪电网络的实际容量对容量进行采样并适当放大，生成具有不同通道容量的网络结构。对于闪电网络子网，将闪电网络中的传输时延设置在 20 ms。为了评估不同调度策略的性能，使用 Python 的 SimPy<sup>[25]</sup>构建了一个带有缓冲区支持的支付通道的离散事件模拟器。该模拟器允许对初始通道余额、通道两侧的交易生成分布（频率、数量和最大缓冲时间）、要模拟的总交易以及每个节点所遵循的调度策略进行参数化。将每个节点设置为平均每秒发送 30 个交易，并且交易发送过程服从泊松过程到达。

本文仿真实验使用从 Kaggle 下载的信用卡数据集进行模拟付款。为了评估该实验的有效性，将 PGSD 算法与以下 3 种算法做比较。

1) 无差别调度 (UPS, unbiased priority scheduling)<sup>[26]</sup>。节点沿路由路径分配每个跳的优先级，对交易流没有偏差。

2) 先进后出 (FILO, first-in-last-out)。先到的交易后进行转发。

3) 定期交易处理 (PTP, periodic transaction processing)<sup>[27]</sup>。当缓冲器的交易数量超过某个阈值或达到固定的持续时间时构建一个联盟，实施一个最优的重新排序策略，以最小化总交易成本。仿真主要参数如表 1 所示。

表1 仿真主要参数

参数	数值
节点 $\mathcal{V}$	100
支付通道 $\mathcal{E}$	700
转发费用 $F_x^i$	6, 4, 2
交易金额 $d_x$	10~15
交易路径跳数 $h_p$	3~7
交易个数 $N$	3 000
优先级个数 $k$	3

### 3.2 性能评估

图4给出了不同支付通道容量下4种算法的交易成功率。与其他3种算法相比,本文提出的PGSD算法在不同支付通道容量下均具有更高的交易成功率。在支付通道容量为28时,PGSD算法的交易成功率分别比UPS、FILO和PTP算法高6.32%、5.98%和8.85%。这是由于本文算法通过调整中间用户在其路径上分配的优先级来控制某些交易的转发费用和交易等待时间,从而允许更多的交易实现更快的交易转发。例如,多个并发交易在其路径上共享支付通道。当一个交易被分配给较低的优先级时,其先前在该路径上被占用的高优先级转发能力将被释放。同时,其他并发交易流可以利用释放的资源达到更低的交易转发,从而提高交易吞吐量。

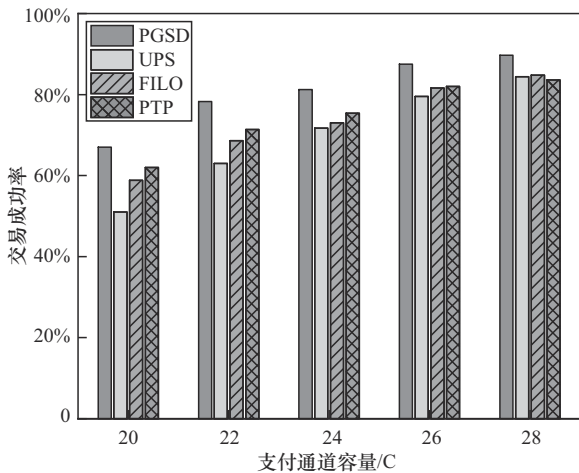


图4 不同支付通道容量下4种算法的交易成功率

图5给出了不同支付通道容量下4种算法的标准化交易吞吐量。随着支付交易通道容量的增加,4种调度算法的标准化交易吞吐量都在增加。这是因为随着支付通道容量的增加,交易可供使用的余

额也增加了,对交易优先级的约束做了一定的松弛。其中,PGSD算法的标准化交易吞吐量始终高于其他算法,在支付通道容量为28时,PGSD算法的标准化交易吞吐量分别比UPS、FILO和PTP算法高6.89%、3.89%和5.56%。此外,当支付通道容量达到26之后,PTP算法的标准化交易吞吐量将超过UPS算法。

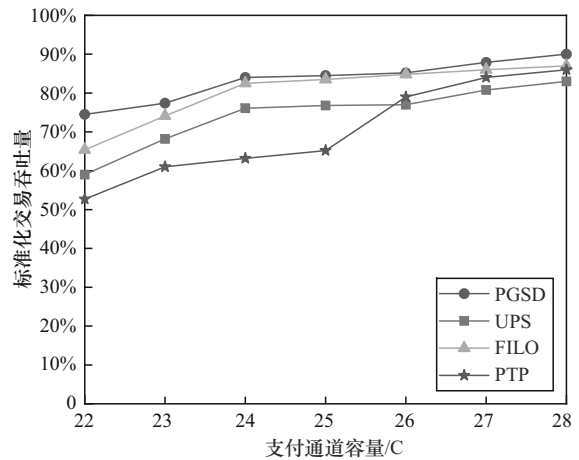


图5 不同支付通道容量下4种算法的标准化交易吞吐量

图6给出了4种算法在不同交易优先级数量下的交易成功率。交易优先级数量越高,交易成功率越低,但PGSD算法的交易成功率始终高于其他3种算法。在交易优先级数量为7个时,PGSD算法的交易成功率分别比UPS、FILO和PTP算法高12.68%、9.15%和19.72%。这是由于在路径转发过程中,遇到的情况越复杂,交易越难以在截止时间内到达终点,选择合适的优先级交易方案也越具挑战。

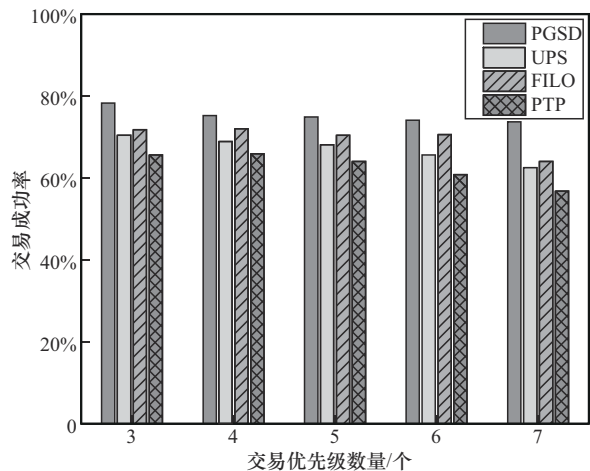


图6 4种算法在不同交易优先级数量下的交易成功率

图 7 给出了 4 种算法在不同交易优先级数量下的平均交易转发费用。由图 7 可知，PGSD 算法的平均交易转发费用始终高于其他 3 种算法。在交易优先级数量为 7 个时，PGSD 算法的平均交易转发费用分别比 UPS、FILO 和 PTP 算法高 47.01%、21.86% 和 13.77%。当交易优先级数量增加时，PGSD 算法的平均交易转发费用逐渐增加，这是由于当交易的截止时间越小且在网络流量大的路径上时，会优先分配优先级最高的情况转发，这导致交易转发费用增加。

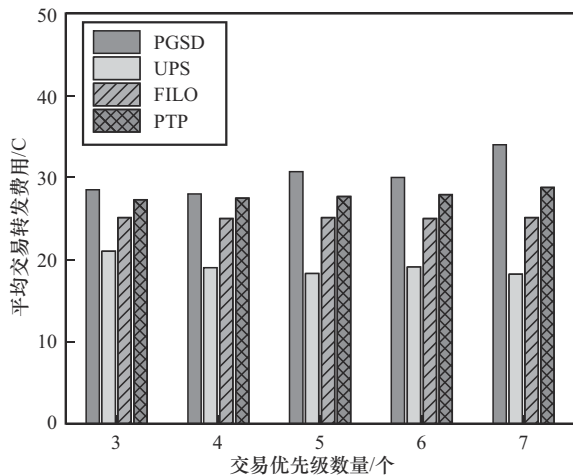


图 7 4 种算法在不同交易优先级数量下的平均交易转发费用

图 8 和图 9 分别给出了 PGSD 算法在不同交易数量下双向和单向交易的总节点初始金额和成功付款的交易金额。随着交易数量的增加，PGSD 算法在双向和单向交易情况下总节点初始金额和成功付款的交易金额均逐渐增加。与单向交易相比，双向交易的总节点初始金额平均低 28.6%，成功付款的交易金额平均高 11.6%，由此可见 PGSD 算法在双向交易情况下的性能优于单向交易情况。因为双向通道在处理反向交易方面具有优势，在支付交易需求越高的情况下，反向交易的可能性越高。进行双向交易有利于处理通道平衡倾斜过大的情况，及时补充通道耗尽的通道防止网络堵塞，提高总交易金额。

图 10 给出了 4 种算法在 Ripple、瓦茨-斯特罗加茨小世界和闪电网络拓扑下的交易成功率。从图 10 可以看到，PGSD 算法的交易成功率始终高于其他 3 种算法，能灵活适应集中化、局部高效和高度分散化等各种不同类型的网络环境。这是因为 PGSD 算法动态地为交易分配优先级，不仅仅考虑交易的

截止时间，还考虑路径上的交易流量大小，为交易选择更加合适的方案。PGSD 算法将转发费用与优先级联系起来，当降低交易优先级时，减少交易在路径转发过程中需要支付的交易转发费用，减轻了交易起点的负担。

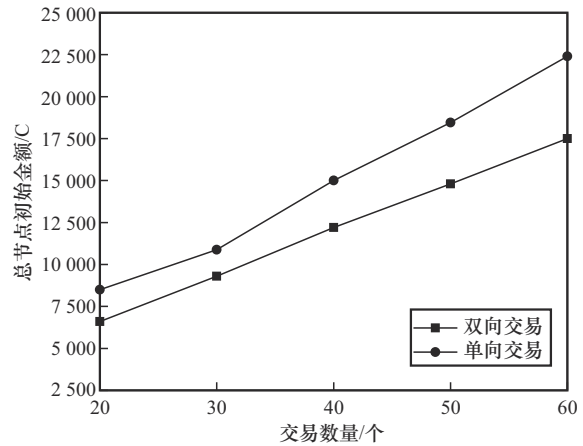


图 8 PGSD 算法在不同交易数量下双向和单向交易的总节点初始金额

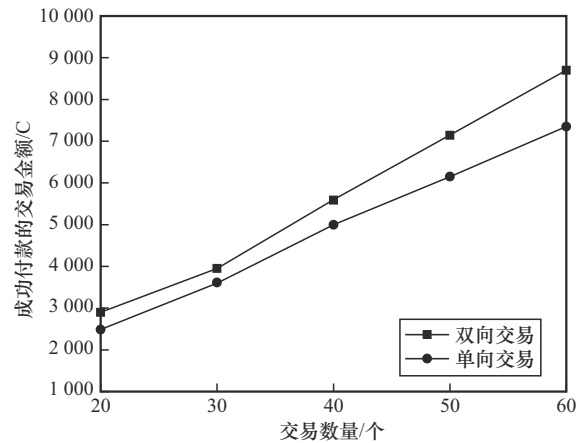


图 9 PGSD 算法在不同交易数量下双向和单向交易的成功付款的交易金额

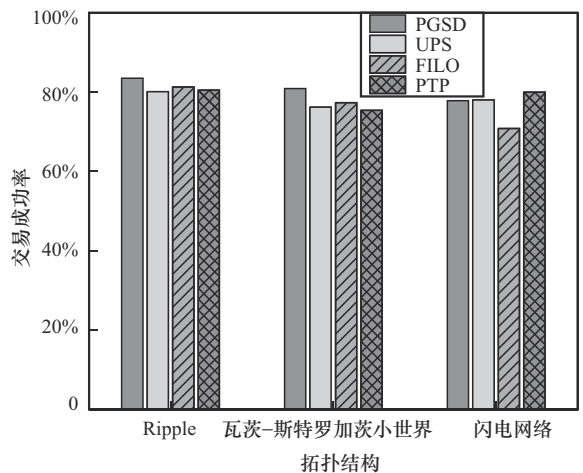


图 10 4 种算法在不同网络拓扑下的交易成功率

## 4 结束语

本文在支付通道网络双向交易场景中综合考虑了交易成功率最大化和节点初始金额最小化的优化问题。在PCN交易路径确定的基础上,本文结合了交易的优先级分配和交易节点转发策略,并考虑了交易的截止时间和通道平衡的限制。为了保证链下交易的顺利执行,本文提出了一种多通道网络博弈框架将分解的2个子问题构建为2个相互关联的博弈,通过2个博弈之间的相互作用进行交易调度策略更新来解决多目标问题。基于Kaggle信用卡数据集的实验表明,本文算法有效降低了交易起始节点金额,并有效提高了交易成功率和网络交易吞吐量。

总体而言,本文方案在提升PCN交易吞吐量方面展现了良好的优化性能。然而在PCN中,交易的完成需要多个参与方协作,包括交易双方、支付通道等。本文缺乏对交易隐私和节点安全的考虑,因此,在未来的研究中,可以进一步探讨交易成功率与交易隐私之间的最佳平衡点,促进链下网络的可扩展性和整体性能的进一步提升。

### 参考文献:

- [1] WANG X J, NING Z L, GUO L, et al. Mean-field learning for edge computing in mobile blockchain networks[J]. *IEEE Transactions on Mobile Computing*, 2023, 22(10): 5978-5994.
- [2] WANG X J, LI T F, XIONG X R, et al. Federation chain for data privacy protection in industrial Internet of things: the perspective from 5G core networks[J]. *IEEE Internet of Things Journal*, 2024, PP(99): 1.
- [3] NING Z L, SUN S M, WANG X J, et al. Intelligent resource allocation in mobile blockchain for privacy and security transactions: a deep reinforcement learning based approach[J]. *Science China Information Sciences*, 2021, 64(6): 162303.
- [4] WANG X J, WANG B B, WU Y, et al. A survey on trustworthy edge intelligence: from security and reliability to transparency and sustainability[J]. *IEEE Communications Surveys & Tutorials*, 2024, PP(99): 1.
- [5] NING Z L, SUN S M, WANG X J, et al. Blockchain-enabled intelligent transportation systems: a distributed crowdsensing framework[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(12): 4201-4217.
- [6] 宁兆龙, 张凯源, 王小洁, 等. 基于多智能体元强化学习的车联网协同服务缓存和计算卸载[J]. *通信学报*, 2021, 42(6): 118-130.  
NING Z L, ZHANG K Y, WANG X J, et al. Cooperative service caching and peer offloading in Internet of vehicles based on multi-agent meta-reinforcement learning[J]. *Journal on Communications*, 2021, 42(6): 118-130.
- [7] WANG X J, ZHU H L, NING Z L, et al. Blockchain intelligence for Internet of vehicles: challenges and solutions[J]. *IEEE Communications Surveys & Tutorials*, 2023, 25(4): 2325-2355.
- [8] 霍如, 倪东, 卢华, 等. 区块链PCN的高效路由策略[J]. *通信学报*, 2021, 42(6): 30-40.  
HUO R, NI D, LU H, et al. Efficient routing strategy of blockchain-based payment channel network[J]. *Journal on Communications*, 2021, 42(6): 30-40.
- [9] 王珺, 马建炜, 罗金喜. 一种应用于边缘计算的区块链分片方案[J]. *物联网学报*, 2023, 7(4): 88-100.  
WANG J, MA J W, LUO J X. A blockchain sharding scheme in edge computing[J]. *Chinese Journal on Internet of Things*, 2023, 7(4): 88-100.
- [10] WANG X J, GU H Y, LI Z Y, et al. Why riding the lightning? Equilibrium analysis for payment hub pricing[C]//*Proceedings of the ICC 2022-IEEE International Conference on Communications*. Piscataway: IEEE Press, 2022: 5409-5414.
- [11] 范伟, 李海波, 张珠君. 区块链数字取证: 技术及架构研究[J]. *通信学报*, 2024, 45(12): 124-141.  
FAN W, LI H B, ZHANG Z J. Blockchain digital forensics: technology and architecture[J]. *Journal on Communications*, 2024, 45(12): 124-141.
- [12] 江沛佩, 王蹇, 陈艳姣, 等. 区块链网络安全保障: 攻击与防御[J]. *通信学报*, 2021, 42(1): 151-162.  
JIANG P P, WANG Q, CHEN Y J, et al. Securing guarantee of the blockchain network: attacks and countermeasures[J]. *Journal on Communications*, 2021, 42(1): 151-162.
- [13] 修佳鹏, 刘卉馨, 杨正球, 等. NDN区块链网络拓扑结构性能分析及优化模型[J]. *通信学报*, 2024, 45(11): 46-58.  
XIU J P, LIU H X, YANG Z Q, et al. NDN blockchain network topology performance analysis and optimization model[J]. *Journal on Communications*, 2024, 45(11): 46-58.
- [14] CHEN W H, QIU X Y, CAI Z T, et al. Graph neural network-enhanced reinforcement learning for payment channel rebalancing[J]. *IEEE Transactions on Mobile Computing*, 2024, 23(6): 7066-7083.
- [15] YU R Z, XUE G L, KILARI V T, et al. CoinExpress: a fast payment routing mechanism in blockchain-based payment channel networks[C]//*Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN)*. Piscataway: IEEE Press, 2018: 1-9.
- [16] ZHANG Y H, YANG D J. RobustPay<sup>+</sup>: robust payment routing with approximation guarantee in blockchain-based payment channel networks[J]. *IEEE/ACM Transactions on Networking*, 2021, 29(4): 1676-1686.
- [17] SIVARAMAN V, VENKATAKRISHNAN S B, RUAN K, et al. High throughput cryptocurrency routing in payment channel networks[C]//*Proceedings of the 17th USENIX Conference on Networked Systems Design and Implementation*. Berkeley: USENIX Association, 2020: 777-796.
- [18] ZHANG X X, QIAN C. Toward aggregated payment channel networks[J]. *IEEE/ACM Transactions on Networking*, 2024, 32(5): 4333-4348.
- [19] WANG W H, MU K, WEI X T. DPCN: towards deadline-aware payment channel networks[J]. *arXiv Preprint, arXiv: 2209.10299*, 2022.
- [20] DONAHUE K, HAUSER O P, NOWAK M A, et al. Evolving cooperation in multichannel games[J]. *Nature Communications*, 2020, 11(1): 3885.

[21] DING K M, ZHANG J S. Multi-party privacy conflict management in online social networks: a network game perspective[J]. IEEE/ACM Transactions on Networking, 2020, 28(6): 2685-2698.

[22] NING Z L, YANG Y X, WANG X J, et al. Dynamic computation offloading and server deployment for UAV-enabled multi-access edge computing[J]. IEEE Transactions on Mobile Computing, 2023, 22(5): 2628-2644.

[23] HU P L, LAU W C. A survey and taxonomy of graph sampling[J]. arXiv Preprint, arXiv: 1308.5865, 2013.

[24] WATTS D J, STROGATZ S H. Collective dynamics of ‘small-world’ networks[J]. Nature, 1998, 393(6684): 440-442.

[25] DU M, YANG P, TIAN W, et al. Anti-collusion multiparty smart contracts for distributed watchtowers in payment channel networks[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3600-3614.

[26] LUO X F, LI P. Learning-based off-chain transaction scheduling in prioritized payment channel networks[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3589-3599.

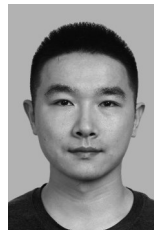
[27] BAI Q L, XU Y D, WANG X. Understanding the benefit of being patient in payment channel networks[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(3): 1895-1908.



唐守泽 (2000-), 男, 山东泰安人, 重庆邮电大学硕士生, 主要研究方向为5G通信网安全。



祝海琳 (1997-), 女, 山东海阳人, 重庆邮电大学硕士生, 主要研究方向为区块链、链下计算等。



周力 (1988-), 男, 湖北汉川人, 博士, 国防科技大学副研究员, 主要研究方向为无线网络、软件定义网络、异构网络。

[作者简介]



王小洁 (1988-), 女, 河北张家口人, 博士, 重庆邮电大学教授, 主要研究方向为无线网络、移动边缘计算、机器学习等。



宁兆龙 (1986-), 男, 辽宁沈阳人, 博士, 重庆邮电大学教授, 主要研究方向为移动边缘计算、应急网络、机器学习、资源管理等。



刘子依 (2001-), 女, 湖南株洲人, 重庆邮电大学硕士生, 主要研究方向为区块链、5G网络安全等。



郭磊 (1980-), 男, 四川眉州人, 博士, 重庆邮电大学教授, 主要研究方向为网络优化、网络通信、光网络等。