



计算机科学

COMPUTER SCIENCE

LN-ERCL闪电网络优化方案

孙敏, 续森炜, 陕童

引用本文

孙敏, 续森炜, 陕童. LN-ERCL闪电网络优化方案[J]. 计算机科学, 2023, 50(11A): 230200115-5.

SUN Min, XU Senwei, SHAN Tong. LN-ERCL Lightning Network Optimization Scheme[J]. Computer Science, 2023, 50(11A): 230200115-5.

相似文章推荐 (请使用火狐或 IE 浏览器查看文章)

Similar articles recommended (Please use Firefox or IE to view the article)

[一种面向多模态医疗数据的联邦学习隐私保护方法](#)

Federated Learning Privacy-preserving Approach for Multimodal Medical Data

计算机科学, 2023, 50(11A): 230800021-8. <https://doi.org/10.11896/jsjcx.230800021>

[一种安全高效的去中心化移动群智感知激励模型](#)

Safe Efficient and Decentralized Model for Mobile Crowdsensing Incentive

计算机科学, 2023, 50(11A): 221000184-10. <https://doi.org/10.11896/jsjcx.221000184>

[基于I-SM4和SM2的混合加密算法](#)

Hybrid Encryption Algorithm Based on I-SM4 and SM2

计算机科学, 2023, 50(11A): 221100116-4. <https://doi.org/10.11896/jsjcx.221100116>

[一种基于纠删码的区块链账本分组存储优化方法](#)

Grouping Storage Optimization Method for Blockchain Ledger Based on Erasure Code

计算机科学, 2023, 50(10): 350-361. <https://doi.org/10.11896/jsjcx.220800193>

[基于本体推理的智能合约漏洞检测系统](#)

Smart Contract Vulnerability Detection System Based on Ontology Reasoning

计算机科学, 2023, 50(10): 336-342. <https://doi.org/10.11896/jsjcx.220900183>

LN-ERCL 闪电网络优化方案

孙敏 续森炜 陕童

山西大学计算机与信息技术学院 太原 030000

摘要 近年来区块链发展迅速,交易频率低成为限制区块链进一步发展的障碍。闪电网络作为解决区块链交易频率问题的最优解决方案之一,具有确认时间短、费用低的优点;但也存在着通道容量低、路由代价大、通道易发生拥堵的问题。现有优化方案多是采用第三方托管,延长交易等待时间,但不能从根源解决通道拥堵问题。针对上述问题,文中提出了一种新的闪电网络优化方案。首先在闪电网络内设置超级节点,并赋予超级节点代币用于相互构建通道,用户通过 Ethereum Request for Comment 标准将比特币转化为代币进入闪电网络;其次提出逃逸值概念,用户节点通过逃逸值计算选择加入一个超级节点;最后改进 landmark 算法对网络通道进行修剪,提升网络可扩展性,解决通道拥堵问题。仿真结果表明,此方案对闪电网络内交易量较大时的网络拥堵、路径寻优时间长等问题有良好效果。

关键词: 区块链; 闪电网络; Landmark; 链下交易; 超级节点; 隐私保护

中图法分类号 TP393

LN-ERCL Lightning Network Optimization Scheme

SUN Min, XU Senwei and SHAN Tong

College of Computer and Information Technology, Shanxi University, Taiyuan 030000, China

Abstract In recent years, blockchain has developed rapidly, and low transaction frequency has become an obstacle to the further development of blockchain. Lightning network, as one of the best solutions to the problem of blockchain transaction frequency, has the advantages of short confirmation time and low cost. However, there are also problems such as low channel capacity, high routing cost and channel congestion. Most of the existing optimization schemes use third-party custody to extend the transaction waiting time, but they cannot solve the channel congestion problem from the root. To solve these problems, this paper proposes a new lightning network optimization scheme. First, set up super nodes in the lightning network, and give super node tokens for mutual channel construction. Users can convert bitcoin into tokens through Ethereum Request for Comment protocol to enter the lightning network. Secondly, the concept of escape value is proposed. The user node chooses to join a super node by calculating the escape value. Finally, the improved landmark algorithm prunes the network channels, improves the network scalability, and solves the channel congestion problem. Simulation results show that this scheme has a good effect on network congestion and long path optimization time when the transaction volume in the lightning network is large.

Keywords Blockchain, Lightning network, Landmark, Off chain transaction, Super node, Privacy protection.

1 引言

近年来随着公民隐私保护意识的提升,区块链被广泛用于不同领域。但是交易确认时间长、交易性能低成为了限制区块链进一步发展的最大阻碍。研究人员就如何提高区块链的交易性能提出了多种优化方案^[1],如分片处理(sharding)、侧链交易、支付通道网络(闪电网络/雷电网络)、优化共识算法等。其中闪电网络(Lightning Network, LN)^[2]是目前解决该问题的最优方案之一。它是支付通道网络(PCN)^[3]构建的一个链下解决方案,通过多重签名技术建立快速支付通道,使交易双方快速结算而无须提交给区块链进行交易确认。

目前,研究人员对闪电网络的研究还处于初步阶段,主要

通过基于信誉的方法、基于地标的方式和遗传算法对闪电网络性能进行优化,但闪电网络仍存在有待改进的问题,如交易通道容量小导致交易拥堵、路径搜索时路径规划非最优路径、网络资金分散、通道冗余等问题。为提升闪电网络的性能, Malavolta 等^[4]提出了一种基于地标的路由协议,通过此协议完成闪电网络中的资金转移,保持闪电网络内部稳定; Thakur 等^[5]通过允许地标在构建各自的根树时进行协调,来保持网络中交易的平衡,提高交易成功率,但失去了去中心化的原则; Stasi 等^[6]提出了基于原子的多路径支付方式,降低了用户支付的费用,增强了闪电网络的可用性; Wu 等^[7]提出了基于本地池化算法^[8]的超级节点清算方案,将小节点资金汇集到超级节点进行交易,增强网络中小节点的清算,并对网络进行本地池化,显著增强小结点清算能力,不能保证对小

基金项目:山西省基础研究计划项目(20210302123455,201701D121052)

This work was supported by the Shanxi Province Basic Research Program, China(20210302123455,201701D121052).

通信作者:孙敏(minsun@sxu.edu.cn)

节点的信息隐私。Burchert^[9]提出支付通道工厂概念,其位于区块链和支付通道网络之间,实现通道的快速关闭。但目前研究方案面对闪电网络节点的成倍增加,短时间内产生大量交易的情况会导致通道堵塞,交易成功率不高。

为解决交易时存在的通道堵塞问题,提升交易成功率,本文提出了一种通过 Ethereum Request for Comment(ERC20)标准^[10]和 Landmark 算法^[11]优化的闪电网络优化方案(Lightning Network Optimization Scheme Optimized by ERC and Landmark Node, LN-ERCL)。该方案通过 ERC 标准完成网络内的资金转换,构建超级节点并互相连接拓宽关键通道的容量;提出了逃逸值概念,对新节点进行分类;改进 Landmark 算法对网络通道进行修剪,并通过仿真实验验证其可行性。

2 引言

2.1 闪电网络基本原理分析

2.1.1 闪电网络原理

闪电网络是一个分布式支付通道网络,其本质上是使用了序列到期可撤销合约(Revocable Sequence Maturity Contract, RSMC)和哈希时间锁定智能合约(Hashed Timelock Contract, HTLC)^[12]来安全地进行零确认交易的一种机制。LN 主要包括 4 个阶段:网络构建阶段、路径查找阶段、交易阶段、通道取消阶段。

1) 网络构建阶段

交易双方通过多重签名技术构建支付通道,多个通道互相连接组成闪电网络。

2) 路径查找阶段

网络上所有的节点通过 Dijkstra 算法计算各自的路由信息,并记录在本地。并向网络发布自己路由信息和资金限制形成支付通道表。

3) 交易阶段

交易的发起方通过支付通道表来判断双方是否有通路,并计算起点到终点的路径,指定交易通过该路径执行。同时,利用洋葱路由^[13]的机制,使得每一个路由节点都只知道相邻的节点,无法了解整条路径,由此达到保护隐私的目的。

4) 通道取消阶段

每次发生交易时,通道内的资金均由双方通过 RSMC 进行确认,并生成带有时间戳的合同。任何一方想要退出通道时,可以将他手中双方签署过的最新交易合同提交到区块链网络中,完成确认后取消通道,通道资金将按照交易合同分配到双方账户中。

2.1.2 闪电网络原理

当交易额大于闪电网络通道宽度时,闪电网络会通过多路径进行交易。图 1 给出了 LN 跨通道交易和多路径支付交易的具体过程。

1) 跨通道交易

LN 支持两个非邻居节点(见图 1(a)中的 A, C)或两个通道资金不足的邻居节点(见图 1(b)中 A, C)跨通道交易。(a)中 A 向 C 发送 4 比特币(BTC)时, A 通过 HTLC 发送 4BTC 给 B,同时 B 发送给 C 4BTC,在 C 收到并确认后, A 提供签名

解锁发送给 B 的 4BTC;完成交易。

2) 多路径支付

当交易路径通道余额不足时,节点可以对交易资金进行拆分,将大额交易资金通过多条路径切割成小额度支付完成交易。图 1(b)中 A 向 C 交易 4BTC 时,首先利用通道③交易 2BTC,剩余 2BTC 经通道①、通道②跨节点完成。

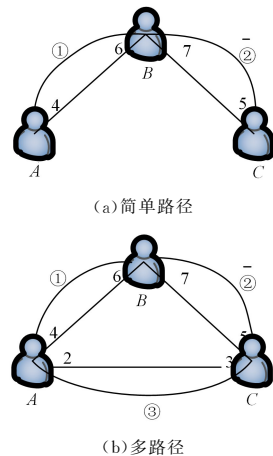


图 1 简单路径和多路径中的金额转换

Fig. 1 Amount transfer method in simple path and multipath

2.2 闪电网络的缺点

闪电网络路由和交易路径确认均通过算法进行选择。根据无免费午餐定理(No Free Lunch Theorem)^[14]可知,在有限搜索空间内,没有任意一种算法能够在优于其他算法的情况下解决所有优化问题。下述是闪电网络交易存在的。

1) 影响交易成功率的关键因素是通道容量的大小。通道容量是随机的,在交易过程中大量交易额度通过小通道时,会使通道发生拥堵,导致交易失败。

2) LN 的路由是通过 Dijkstra 算法进行计算的,当网络规模变大时,完成路由所需时间会大幅度增加,不利于网络的扩展。

2.3 Landmark 算法原理

Landmark 算法以 landmark 节点为根节点构造整个网络的生成树,通过生成树的搜索确定路径的多路由由算法。算法中可以有多个 landmark 节点;当选取一个 landmark 节点时,只有一棵树提供路径搜索服务,类似于单路路由;当有多个 landmark 节点时,不同生成树中的多条路径共同提供路由服务。算法的流程如下。

1) landmark 节点选取:依据节点连通度大小、可信程度等因素,以随机抽取的方式选取 landmark 节点。

2) 生成构造树:采用 BFS 算法构造全网生成树。

3) 可达路径搜索:在所有生成树中搜索从发送方经过 landmark 节点到接受方的可达路径。

4) 可用路径计算:在可达路径的基础上增加对通道容量、处理时间等方面的需求,计算出可用路径集合。

5) 交易多路执行:发送方基于可用路径集合,确定拆分策略与路由路径,完成交易。

3 LN-ERCL 闪电网络优化方案

为解决 2.2 节中存在的问题,本文提出了一种 LN-ERCL 的优化方案,图 2 给出了 LN-ERCL 方案的流程图。

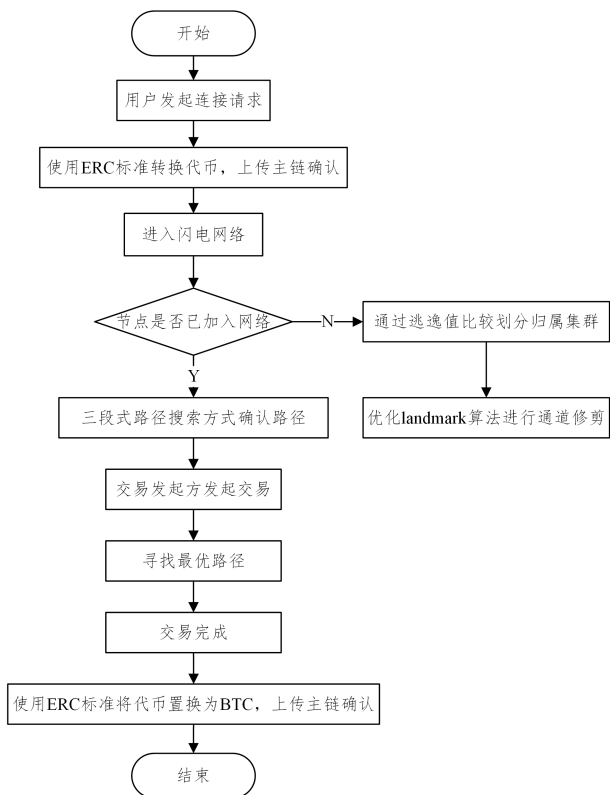


图 2 LN-ERCL 方案交易的流程图

Fig. 2 Transaction flow chart of LN-ERCL scheme

3.1 预处理和输出

WBTC 将比特币标准化为 ERC20 格式,为比特币创建智能合约,加快比特币网络的处理速度。为了拓宽通道容量,本方案使用 ERC20 标准接口转换资金(下文称作代币),并通过智能合约在闪电网络中生成节点,将生成的初始代币传入节点地址中,这些节点被命名为超级节点。

超级节点通过以下两点保证其安全性。

1)通过智能合约的设置使超级节点不能主动发起任何交易,仅能在交易中充当桥梁作用。

2)为了保证超级节点内代币不被第三方盗用,超级节点资金经 ERC 协议监控,网络内所有的用户节点均可以查看超级节点及其通道的资金数量,以此进行监管,保证用户的资金安全。

3)防止超级节点作恶的方法:对交易合同的时间锁和多签名机制进行监管,出现超时或签名异常时交易双方均可选择取消交易,代币数量将通过交易合同返回交易前状态。为防止节点无成本取消交易,恶意占用通道,交易占用通道产生的 gas 费用将由取消交易的一方承担。

3.2 超级节点网络构建方法

设立逃逸值参数对节点资金进行判断,通过计算节点逃逸值选择加入合适的集群。节点进入网络的方法如算法 1 所示。

算法 1 网络构建算法

输入: $r_1+R; num;$

输出: ID;

1. 初始化逃逸值参数: $Escape\ T \leftarrow \emptyset;$ /* T 为逃逸值参数集 */

2. 初始化:

for $i \leftarrow 0$ to num /* num 为通道数量 */

$T[i] \rightarrow id \leftarrow ID;$

$T[i] \rightarrow num \leftarrow r(i);$

3. 合并 ID 相同项的数据: $merge(\&T);$

4. if $T \rightarrow id = ID$

$T \rightarrow num += RID;$

5. 设置排斥值 S , 限制资金上限:

If $T \rightarrow num > S$

$T \rightarrow num \leftarrow 0;$

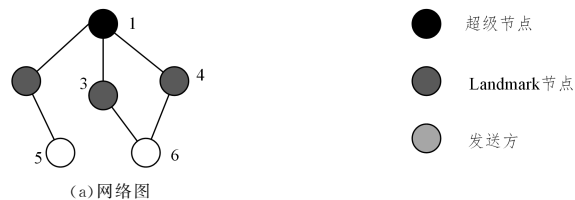
$T \leftarrow \max(T \rightarrow num);$

6. 输出结果: $return\ T \rightarrow id;$

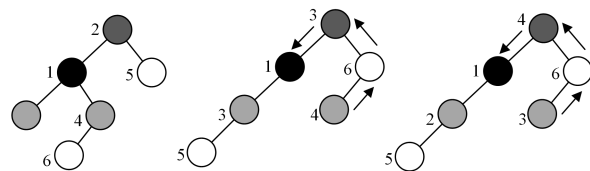
3.3 网络内的通道构建方法

现有的闪电网络路径搜索方案一般通过 Dijkstra 算法进行全局搜索,搜率效率低,代价大。通过以多个超级节点为中心将闪电网络切割成若干子网络,对子网络内的路径进行搜索,减小节点间路径搜索的代价。

Landmark 算法是一种基于预处理的 shortest path 算法,通过预处理一些特殊的节点,即 Landmark 节点,来加速最短路径的查询。它的优势在于解决路由选择中心化、通道阻塞严重等问题^[15]。Landmark 节点的选取方法和数量对算法的效率和准确性有很大影响。Landmark 节点应选取覆盖范围广、代表性强的节点。本文通过基于中心性的思想对选取范围进行修改,以适应本文特殊的网络结构。



(a) 网络图



(b) landmark 节点为根的生成树

图 3 Landmark 算法的路径搜索

Fig. 3 Path search of Landmark algorithm

Step1 由于节点均匀分布在子网络中,因此节点的大部分交易是跨子网络交易,必须经过超级节点。故选取超级节点的邻接点作为 landmark 节点的选取范围。

Step2 通过 BFS 遍历图 3(a)图,生成邻接点集 edge,即为 landmark 节点可选取集;landmark 节点数量不能超过子网络的 5%,根据节点资金量降序选择 landmark 节点。

Step3 分别将邻接点设定为 landmark 节点对子网络进行预处理,将最优路径保存在 pri 中,遍历所有节点最终形成子网络的最优路径表,并将其保存在本地。图 3(b)以 landmark 节点为根,通过 BFS 搜索得到的生成树,超级节点始终是根节点的孩子节点。查询到超级节点的最优路径只需查询点到根节点的最优路径即可。

Step4 将未存在于 pri 的边缘通道关闭,完成通道修剪。减少子网络的冗余,提升网络的可扩展性。

LN-ERCL 方案的路径搜索方式分为 3 段:1)节点的到超级节点的路径;2)超级节点间的路径;3)超级节点到交易接收方的路径。搜索结果保存在本地并上传网络形成支付通道表,能有效缩短路径搜索时间。

4 仿真实验

为了验证本文提出方案的优越性能,我们对真实闪电

网络^[2]、基于超级节点的本地池化网络^[16]与 LN-ERCL 方案进行了对比。本文使用 CLoTH 闪电网络模拟器^[17]进行仿真模拟。

4.1 参数设置

由文献^[17]可知,2021 年 1 月闪电网络内比特币数为 2455 枚,截至 2022 年 10 月网络内比特币达到 4750 枚。本文参考文献^[17]中的各项数据和实际增幅进行模拟实验环境设置,具体参数如表 1 所列。

表 1 模型参数设置
Table 1 Model parameter setting

参数名	参数值
payment_rate/交易速率//s	1000
n_payments/交易数量	10^5
average_payment/平均通道容量	$5 * 10^5$
n_nodes/节点数量	6500
n_channels_per_node/节点平均通道数量	6
average_payment_amount/平均交易额	10^4
Super_node/超级节点通道容量	$5 * 10^6$

4.2 实验环境

为测试 LNERCL 方案的性能实验,实验选用操作系统:Linux(64 位);CPU 为 Intel(R)Core(TM)i5-6300HQCPU@2.30GHz 2.30GHz;运行内存为 8GB;python 版本为 python3.7。

4.3 性能指标

在交易过程中,对闪电网络性能进行评价的指标有交易成功率、交易失败率(包括节点间通道容量不足导致失败和节点无可用路径导致失败)、路径搜索时间、交易完成时间。为保证结果的普遍性,实验结果使用 5 次实验的平均值。成功率和失败率计算式如下:

$$Success = \frac{SN}{TN} \quad (1)$$

$$Failure = \frac{FN}{TN - SN} \quad (2)$$

其中,Success 和 Failure 是交易完成后的成功率和失败率;TN 是交易总量,SN 是交易成功的数量,FN 是交易失败集合中特定失败因素的数量。

4.4 消融实验分析

构建网络后修剪通道对网络通道数量和搜索时间进行分析,表 2 列出了进行消融实验后的结果。

表 2 消融实验时间的对比
Table 2 Comparison of ablation test time

节点数量 * 10^3	剔除修剪操作 的通道数量	剔除修剪操作 路径搜索时间/s	进行修剪后 通道数量	修剪路径 搜索时间/s
5	24512	0.646	21003	0.513
6	29447	0.815	25328	0.658
7	33795	1.265	28928	0.962
8	39512	2.063	33142	1.619
9	45886	3.462	38124	2.845
10	50121	6.251	42753	4.012

数据显示剔除通道修剪操作后,通道数量随节点数量的增长量远高于修剪后的数量;同时使用修剪操作的路径搜索时间比剔除修剪操作的时间短 20%~40%,随着节点数量增多,修剪操作的优化会进一步体现,能有效提升网络维护代价以及减少路径搜索时间。

4.5 算法时间复杂度分析

Dijkstra 算法的时间复杂度为 $O((E+V)\log V)$,其中 E 是边的数量, V 是节点的数量。参考 4.1 节,选取 $E=2^{17}$,

$V=2^{15}$ 。Dijkstra 算法的计算次数为 $15 * (2^{15} + 2^{17})$ 。

Landmark 算法的时间复杂度为 $O(kv\log(v) + (E/(nk)\log k))$,其中 k 是 landmark 的数量, n 是超级节点的数量, v 是子网络节点数量 $v=V/n$ 。Landmark 算法的时间复杂度由两部分组成:(1)预处理,即计算每个顶点到 landmark 的最短距离,时间复杂度为 $O(kv\log v)$;(2)查询,即对每个查询计算起点到终点的最短距离,时间复杂度为 $O((E/nk)\log k)$ 。因此,Landmark 算法的总时间复杂度为 $O(kv\log v + (E/nk)\log k)$ 。Landmark 节点不超过 5%,为方便计算选取最接近的 2 的倍数 $k=2^8$;实验中超级节点数量约为节点数的 1/1000, $n=2^5$; $v=2^{10}$ 计算次数为 $8 * 2^{18} + 5 * 2^4$ 。可以看出,在当前节点数量的情况下,landmark 算法的时间复杂度低于 Dijkstra,若节点数进一步增长,landmark 算法的时间优势会进一步体现。

4.6 仿真实验结果

交易成功率是评价方案最重要的指标。图 4 给出了 3 种网络在不同交易量下的交易成功率。平均交易额 $\in [1000, 5000]$ 时,拥有超级节点的方案的交易成功率明显高于实际网络。平均交易额 $\in [5000, 10000]$ 时两种对比方法的交易成功率明显降低,LN-ERCL 方案的成功率高于对比方案 10%~28%。

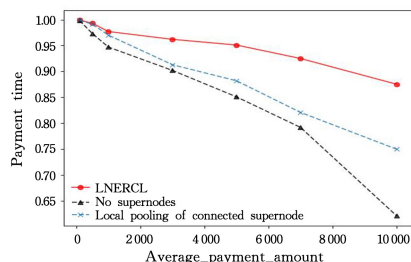
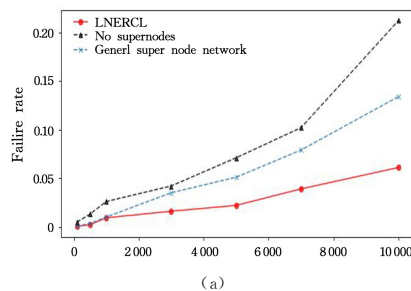


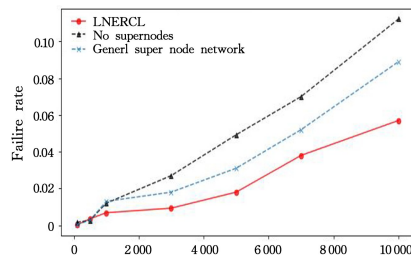
图 4 交易成功率对比

Fig. 4 Comparison of transaction success rate

FailNoPath 和 FailNoBalance 是造成交易失败的两个主要因素。图 5(a)、图 5(b)分别是 3 种模型中 FailNoPath 和 FailNoBalance 造成交易失败的概率对比图。



(a)



(b)

图 5 交易失败率对比

Fig. 5 Comparison of transaction failure rate

图 5(a)中,优化后模型 FailNoPath 的失败率始终低于原

网络模型和一般超级节点网络,在大额度交易情况下 LN-ERCL 方案的平均失败率比其他方案低 4%~16%;图 5(b) 中,在大额交易量下, LN-ERCL 有明显优势,平均失败率对比模型低 4%~6%。

图 6 给出了模拟路径搜索时间, LN-ERCL 方案经三段式路径搜索方式的时间低于其余两种方案路径。特别是在节点数超过 9000 时,本方案时间成本与对比实验差距进一步拉大。此结果表明,在闪电网络规模扩大时,本方案对降低路径搜索的时间成本有良好效果。

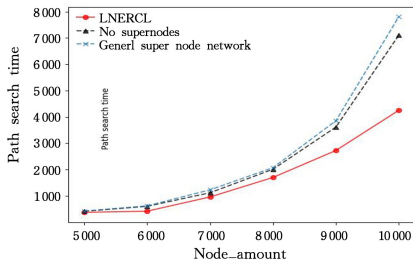


图 6 模拟路径搜索时间

Fig. 6 Simulation time of node path search

模拟交易时间指不同方案模拟 10^5 次交易的时间。如图 7 所示,随着交易量增大,本方案的交易时间始终低于对比实验方案。在大量交易的情况下,本文方案的交易堵塞率低的优势得以体现,使完成交易时间低于其他对比实验。

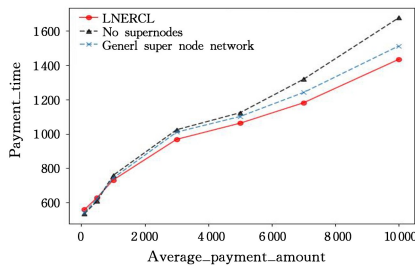


图 7 模拟交易时间对比

Fig. 7 Comparison of simulated transaction time

综上,本文提出的 LN-ERCL 方案通过提高交易的成功率,降低路径搜索时间和交易时间的方式,提升了闪电网络的可用性和可扩展性。

结束语 本文提出了 LN-ERCL 方案,用于优化闪电网络。通过 ERC 协议铸造代币,使生成的超级节点可以构建大容量通道,通过提出逃逸值概念使节点加入网络,维持网络内各集群间的平衡;改良 Landmark 节点的选取范围以优化寻优路径,并去除边缘通道,解决了 LN 内高交易量状态下路径搜索时间过长和通道堵塞的问题。实验结果证明,该方案对缩短搜索时间和减小通道堵塞概率有明显作用。在未来工作中着重优化网络内路径搜索算法和可达路径选择方式,减小路由代价,提升网络的可扩展性。

参考文献

[1] LI W, HE M, HAIQUAN S. An Overview of Blockchain Technology: Applications, Challenges and Future Trends[C]// IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC). 2021: 31-39.

[2] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain lightning network [EB/OL]. [2021-06-09]. <https://lightning.network/lightning-network-paper.pdf>.

ning.network/lightning-network-paper.pdf.

- [3] DECKER C, WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels [C]// Symposium on Self-Stabilizing Systems. 2015: 3-18.
- [4] MALAVOLTA G, MORENO-SANCHEZ P, KATE A, et al. Silent whispers: Enforcing security and privacy in decentralized credit networks[C]// IACR Cryptology ePrint Archive 2016. 2016: 1053-1054.
- [5] THAKUR S, BRESLIN J G. Coordinated Landmark-based Routing for Blockchain Offline Channels[C]// 2022 Second International Conference on Blockchain Computing and Applications (BCCA). 2022: 108-114.
- [6] STASI G D, AVALLONE S, AL. Routing Payments on the Lightning Network[C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber. 2018.
- [7] WU J, JIANG S. On Increasing Scalability and Liquidation of Lightning Networks for Blockchains[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(4): 2589-2600.
- [8] WU J, DAI F. A generic distributed broadcast scheme in ad hoc wireless networks[J]. IEEE Transactions on Computers, 2004, 53(10): 1343-1354.
- [9] BURCHERT C, DECKER C, WATTENHOFER R. Scalable funding of bitcoin micropayment channel networks[J]. Royal Society Open Science, 2018, 5(8): 180089.
- [10] ANGELO M, DSALZER G. Tokens Types and Standards: Identification and Utilization in Ethereum[C]// 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS). 2020.
- [11] TSUCHIYAP F. The landmark hierarchy: A new hierarchy for routing in very large networks[J]. ACM SIGCOMM Computer Communication Review, 1988, 18(4): 35-42.
- [12] WIKIB. Hash time locked contracts[EB/OL]. https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts.
- [13] GOLDSCHLAG D M, REED M G, SYVERSON P F. Hiding routing information[C]// Information Hiding. Berlin, Heidelberg: Springer, 1996: 137-150.
- [14] WOLPERT D H, MACREADY W G. No free lunch theorems for optimization [J]. IEEE Transactions on Evolutionary Computation, 1997.
- [15] JIA L P, PEI Q, WANG X, et al. Survey on Offchain Channel Routing Algorithm[J]. Journal of Software, 2022, 33(1): 233-253.
- [16] WU J, JIANG S. Local Pooling of Connected Supernodes in Lightning Networks for Blockchains[C]// 2020 IEEE International Conference on Blockchain (Blockchain). 2020: 421-427.
- [17] CONOSCENTI M, A VETRÒ, MARTIN J. CLOTH: A Lightning Network Simulator[J]. Simulation Modelling Practice and Theory, 2021, 15: 100717.



SUN Min, born in 1966, master degree, professor. Her main research interests include computer network and information security.