软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(10):3858–3873 [doi: 10.13328/j.cnki.jos.006380]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链闪电网络实证分析: 拓扑、发展和收费策略*

陈艳姣[1], 朱笑天[1], 于永瑞[1], 程子英[2]

[1](武汉大学 计算机学院, 湖北 武汉 430072)

[2](武汉大学 数学与统计学院, 湖北 武汉 430072)

通信作者: 陈艳姣, E-mail: chenyj.thu@gmail.com

摘 要: 比特币闪电网络作为最广泛使用的支付通道网络之一, 自其 2016 年提出就引起了广泛关注. 支付通道网络是一种用以解决区块链可扩展性问题的 Layer-2 技术. 在支付通道网络中, 参与者只需在区块链上提交开通和关闭支付通道的 Layer-1 事务, 就可以在链下完成多笔支付交易. 这一工作机制既避免了等待每笔交易被验证的时间耗费, 同时也节省了交易费用. 然而, 由于闪电网络投入使用的时间较短, 以往的相关研究都是基于有限的、闪电网络仍处于快速发展时期的数据, 缺乏必要的时效性. 为了填补这一空白, 全面了解闪电网络的拓扑结构及其发展趋势, 基于更新至 2020 年 7 月、具有高时效性的数据, 采用图分析的方法描述闪电网络静态和动态的特征. 同时对网络中节点进行聚类分析, 并从聚类结果中得到了一些结论. 此外, 通过比较链上和链下的交易费用, 对闪电网络的收费机制作了更进一步的研究.

关键词: 区块链; 比特币; 闪电网络; 支付通道网络; 网络拓扑结构

中图法分类号: TP309

中文引用格式: 陈艳姣, 朱笑天, 于永瑞, 程子英. 区块链闪电网络实证分析: 拓扑、发展和收费策略. 软件学报, 2022, 33(10): 3858–3873. http://www.jos.org.cn/1000-9825/6380.htm

英文引用格式: Chen YJ, Zhu XT, Yu YR, Cheng ZY. Empirical Analysis of Lightning Network: Topology, Evolution, and Fees. Ruan Jian Xue Bao/Journal of Software, 2022, 33(10): 3858–3873 (in Chinese). http://www.jos.org.cn/1000-9825/6380.htm

Empirical Analysis of Lightning Network: Topology, Evolution, and Fees

CHEN Yan-Jiao[1], ZHU Xiao-Tian[1], YU Yong-Rui[1], CHENG Zi-Ying[2]

[1](School of Computer Science, Wuhan University, Wuhan 430072, China)

[2](School of Mathematics and Statistics, Wuhan University, Wuhan 430072, China)

Abstract: Being one of the most deployed payment channel networks (PCN), the lightning network (LN) has attracted much attention since it was proposed in 2016. The LN is a layer-2 technology addressing the scalability problem of bitcoin. In LN, participants only need to submit layer-1 transactions on the blockchain to open and close the payment channel, and they can issue multiple transactions off-chain. This working mechanism avoids the waste of time on waiting for every transaction to be verified and simultaneously saves transaction fees. However, as the time of LN put in practice is rather short, previous works were based on small volume and rapidly-changing data, which lacks necessary time-effectiveness. To fill in the gap and get a comprehensive understanding of the topology of LN and its evolving trend, this study characterizes both static and dynamic features of LN by leveraging graph analysis based on data of high time-effectiveness updated to July, 2020. A clustering analysis of the nodes is carried out, and some conclusions and insights derived of the clustering results are presented. Moreover, an additional study of the charging mechanism in LN is conducted by comparing the on-chain and off-chain transaction fees.

Key words: blockchain; bitcoin; lightning network (LN); payment channel network; network topology

区块链技术自诞生以来, 就以其开放、去中心化、可公开验证等特性备受欢迎. 然而, 随着参与人数的激

* 基金项目: 国家自然科学基金(61972296)

收稿时间: 2020-12-09; 修改时间: 2021-03-15; 采用时间: 2021-05-19; jos 在线出版时间: 2021-08-03

增, 区块链系统中的一些问题逐渐暴露出来. 因其无需许可和去中心化的特性, 比特币系统平均挖矿时间为每个块 10 分钟, 且每秒最多只能处理 7 笔交易. 这样的性能显然无法满足比特币市场上日益增长的交易需求. 此外, 由于比特币挖矿过程与交易的金额无关, 这意味着在其他相关因素相同的情况下, 不同交易金额的交易所要支付的交易费用是相同的. 显然, 这种收费机制对于小额交易来说十分不经济. 为了解决上述问题, 支付通道网络(payment channel network, PCN)应运而生. 不久后, 闪电网络(lightning network, LN)[1]作为一种支付通道网络, 被部署在比特币系统上.

由于主流加密货币(例如比特币和以太坊)的去中心化本质极大地阻碍了其交易吞吐量, 支付通道网络成为解决区块链可扩展性问题和高昂的交易费用问题的有效途径. 支付通道可被理解为是一个交易双方的账本, 由两位用户自行建立和维护. 交易双方无需向区块链报告每一笔具体的交易, 只需将开通和关闭支付通道的事务提交到区块链上, 以保障链下交易安全, 使得交易双方能够取回自己的合法资金. 开通支付通道时, 两位用户需在区块链上进行存款操作, 锁定其抵押资金作为链下账本的初始资金. 在之后的交易中, 双方通过链下消息发布账本余额变化, 进行转账. 当双方达成协议, 决定关闭该交易通道时, 账本中记录最新的通道余额分配状态会被报告给区块链, 双方进而可以取回其应得的合法资金. 在多个支付通道组成的支付通道网络中, 用户不仅能和与其直接相连的用户进行交易, 还能和与其间接相连的用户进行交易, 这样的过程涉及多个用户参与的多跳交易. 总而言之, 由于链下的支付通道网络可以进行大量实时的交易, 极大地提高了交易的吞吐量; 同时, 支付通道网络中的交易费用与区块链上的交易费用相比微不足道.

闪电网络作为基于比特币系统的支付通道网络, 是目前被最广泛使用和研究的支付通道网络. 除了上文所述的运行机制外, 闪电网络采用特定的智能合约来确保其运作. 例如: RSMC (revocable sequence maturity contract)机制确保资金只能经过交易双方的同意或预先拟定的退款程序退还, 并且只接收链下账本中余额分配的最新状态; HTLC (hashed time lock contract)机制通过引入 nLockTime 概念来处理多跳交易, 以确保交易的原子性. 然而, 闪电网络的蓬勃发展也逐渐暴露出一些问题. 例如, 人们会担心闪电网络中是否会出现超级中心节点, 破坏其去中心化的属性. 此外, 如何在闪电网络中寻找最有效且经济的支付路由, 也是一个重要问题. 这些问题都与闪电网络静态和动态的拓扑特征密切相关.

虽然闪电网络投入使用距今不到 3 年, 但学术界已有许多相关研究[2−7]. Martinazzi 等人[3]研究了闪电网络的拓扑特征演化及其效率和同步性, 并涉及了安全问题. 文献[4]量化了闪电网络对基于拓扑结构的攻击的抵抗能力. 然而, 这些研究都有很强的时间局限性. 文献[2–4]均使用了 2018 年 2 月–2019 年 1 月约 1 年时间的闪电网络通道数据, 在这段时间内, 闪电网络仍处于刚起步的快速发展阶段, 数据缺乏必要的时效性. 在这一阶段, 人们往往出于好奇而试探性地使用闪电网络, 其相关的数据分析十分有限, 不足以反映闪电网络趋于稳定发展阶段后的特性. 除上述方面外, 闪电网络中的路由问题也具有重要的研究价值. Flare[5]是当前闪电网络的路由方法, 用以尽快找到支付路径. 一些研究者还提出了其他新颖的路由方法. 例如, 文献[6]中提出的多径路由支付方案, 大大降低了交易的费用. 此外, 还有一些关于闪电网络中交易仿真的研究, Béres 等人[7]为闪电网络设计了一个用于分析不同节点的路由成本和潜在收益的流量模拟器.

本文旨在全面、系统地了解闪电网络, 以期解决闪电网络中存在的一些问题. 因此, 本文全面分析了闪电网络的拓扑特征、发展趋势及其收费机制. 基于截至 2020 年 7 月更新的通道数据, 对闪电网络的静态和动态特征及其收费策略进行了评估. 本文的研究工作分为 3 部分.

- 第 1 部分关注闪电网络的静态拓扑结构. 通过图分析的方法, 对闪电网络的静态拓扑特征给出全面、细致的解释. 具体来讲, 对闪电网络的重要属性、典型特征的分布进行了分析, 并使用聚类方法探索闪电网络中节点之间的共性;
- 第 2 部分关注闪电网络的动态拓扑变化. 深入研究了闪电网络规模、节点和通道特征的演化趋势, 进而了解闪电网络的发展趋势. 由于闪电网络是在 2016 年[1]设计的, 2018 年 1 月被部署到比特币主网上使用, 其应用时间十分有限. 在此背景下, 与以往针对闪电网络展开的研究相比, 本文更关注闪电网络处于稳定发展阶段的网络特征和发展特性, 结果具有较高的时效性, 且丰富的通道数据也加强了

结论和预测的可靠性;

- 第 3 部分关于闪电网络的收费机制. 在闪电网络中进行模拟交易(一种路由策略以交易费用最小化为目标, 另一种路由策略以路径长度最小化为目标), 以获取不同交易金额下的交易费用, 并对链上的交易费用进行合理估计, 进而比较链上和链下交易费用的差异.

本文的主要贡献如下:

- 基于大量具有高时效性的数据, 对闪电网络的静态和动态拓扑特征进行系统分析. 根据闪电网络的动态拓扑特征, 分析闪电网络的发展趋势;
- 对闪电网络中的节点进行聚类分析, 最终将节点划分为 4 类, 并对聚类结果给出合理的解释和可能的应用情境;
- 深入理解闪电网络的收费策略. 通过对链上和链下交易费用的比较, 对闪电网络的收费机制进行综合分析. 为了得到链下交易费用, 采取交易费用最小化和路径长度最小化两种路由策略进行交易路由的模拟.

1 背 景

1.1 支付通道网络

区块链因其开放、去中心化、可公开验证的特性, 被看作是一种具有颠覆性的创新技术. 然而, 比特币网络的交易广播机制导致其交易吞吐量非常低, 每秒最多只能处理 7 笔交易, 而其他集中支付方法(例如 MasterCard 和 Visa)在高峰时期的交易速度高达每秒 4 万笔. 此外, 比特币链上交易费用对于小额交易来说十分昂贵. 用户无疑希望支付较低的交易费用来完成交易. 所以在比特币交易中, 特别是在小额、高频的交易中, 用户一直都在寻求一种更经济的交易方式. 因此, 研究人员提出了一些方法[7−10], 用以解决上述区块链可扩展性问题, 其中一个很有应用前景的方案是支付通道网络.

支付通道网络作为一种基于区块链的、无需第三方可信机构验证的机制, 使得用户在比特币链下完成交易, 为区块链可扩展性问题和交易费用高昂等问题提供了一个较为理想的解决方案. 支付通道使得链上缓慢、昂贵的交易可以在链下快速、低廉地进行. 交易双方只需在开通和关闭支付通道时与区块链进行交互, 而其他交易可以通过支付通道在链下进行. 交易的安全性通过一些特定的协议(例如 RSMC[1])来保证, 以防止由于一方单方面放弃交易而损害另一方利益的情况发生. 随着参与者和支付通道数的增加, 形成了由节点(参与者)和边(支付通道)组成的网络, 即支付通道网络.

应用支付通道网络进行交易的过程可分为以下 3 个阶段.

(1) 开通支付通道. 开通支付通道的事务是在链上进行的. 在这一阶段, 双方合作开通通道, 并在其中锁定自己的抵押资金. 资金被交付到一个 2-of-2 多重签名地址, 只有在双方签名后才能退还抵押资金或取回交易后的资金;

(2) 进行链下交易. 这一阶段是在链下进行的, 交易双方在支付通道中交换他们的余额. 根据设置的不同, 这个支付通道可以是双向的, 也可以是单向的. 交易细节仅限于交易双方, 即在区块链链上不会有任何链下交易的痕迹. 多重签名机制可以在不公开广播的情况下保证交易的安全性. 双方可以进行多次交易, 并在每次余额分配发生变化时实时更新多重签名地址. 但是, 由于支付通道仍然使用统一签名锁定, 没有人能够取出超出其应得金额的资金, 通道中的余额总额也不会改变. 当双方达成协议不再进行余额转移时, 就进入了下一阶段;

(3) 关闭支付通道. 关闭支付通道的事务是在链上进行的. 在双方对支付通道中的最终余额分配达成共识后, 他们交换彼此的签名, 通过有效的 2-of-2 多重签名在关闭交易中取回各自账户上的资金. 至此, 支付通道得以成功关闭.

1.2 闪电网络

闪电网络是目前最著名的支付通道网络, 它于 2016 年[1]被提出, 并于 2018 年 1 月在比特币主网上发布, 随后吸引了大批参与者加入. 闪电网络作为第一个比特币支付通道网络的应用, 实现了比特币链下交易的总体框架. 除上文中介绍的工作原理外, 本节主要介绍闪电网络中维持交易原子性的协议以及闪电网络的收费机制.

在闪电网络中, 两个不直接相连的节点可以通过中间节点进行多跳交易支付. 例如, Alice 和 Bob、Bob 和 Carol 分别有直接相连的支付通道, Alice 和 Carol 之间无直接相连的支付通道, 但 Alice 和 Carol 之间的交易可以通过 Alice 先转账给 Bob, Bob 再转账给 Carol 来实现. 在多跳交易中, 需特别关注交易的原子性问题. 闪电网络的 HTLC 协议[1]使得多跳交易得以维持原子性. 多跳交易的原子性是指, 当交易的每一跳支付都顺利完成后, 交易所涉及到的所有通道的余额分配都会更新. 然而一旦有一笔支付没有完成, 则该次交易就会被认定为失败, 所有相关支付通道的余额分配均不会发生更改. 交易双方可以在双向的支付通道中安全地进行交易, 但是跨越多个通道进行安全的资金转移需要额外的设计. 闪电网络提出 HTLC 来保障交易的安全性和原子性. 在闪电网络中, 每一跳支付, 中间节点用户在限制时间内, 根据交易对象提供的有关原像 R 的信息来完成哈希值的计算, 进而使交易能够传递到下一跳. 关于原像 R 和哈希值的计算, 继承了区块链工作机制的特性, 从而保证了交易的安全性. 在规定的时间范围内, 交易资金会保持锁定在通道中. 一旦交易的某一跳停止或超时, 本次交易将被取消, 所有通道的状态将恢复到此次交易之前的状态.

关于闪电网络的收费机制, 闪电网络的使用涉及开通和关闭支付通道、进行链下交易等过程. 由于开通和关闭支付通道的过程是在链上进行的, 闪电网络内的支付交易是在链下进行的, 这里, 我们对链上和链下两类交易费用进行了解释.

(1) 链上交易费用. 如第 1.1 节所述, 开通支付通道和关闭支付通道的交易都是在链上完成的, 这意味着这些交易的费用是严格按照区块链的工作机制产生的. 当双方对一个链上交易达成共识时, 他们会将本次交易发布到网络中, 并等待网络中的矿工进行计算来验证交易的正确性. 当交易被打包进区块, 且该区块经过验证被成功添加到主链上后, 双方才会认可本次交易有效. 也就是说, 区块链运行的关键是让网络中所有节点对区块的内容达成一致, 然后将其添加到主链上. 这个过程中, 区块实际上充当了交易的记录簿. 因为验证区块时的计算消耗了电力、计算能力及众多其他资源, 矿工需要金钱奖励去驱动他们进行验证. 因此, 交易双方对交易被验证的需求与矿工通过采矿工作获取利润的意愿进行匹配, 构建了在区块链上进行转移资金的交易方式. 基于以上背景可知: 支付给矿工的交易费用和交易的实际金额无关, 而是与交易广播时区块验证的计算难度有关, 也即与比特币系统在交易时的状况密切相关. 因此, 当交易金额较大时, 单位交易金额对应的交易费用是经济实惠的; 否则, 单位交易金额的交易费用不容小觑;

(2) 链下交易费用. 前文中详细说明了在闪电网络中如何通过中间节点进行多跳交易. 在多跳交易中, 为激励中间节点辅助转移资金, 支付路由成功后, 中间节点可以得到一些奖励, 如一定数额的资金. 这就是链下交易费用的来源. 在闪电网络中, 中间节点具有自己独特的收费策略, 它们可以自行设置两种类型的费用, 即基础费用(base fee)和费率(fee rate). 基础费用是指当有交易经过该中间节点时便会收取的固定费用. 费率是一个比率, 代表每转移 1 sat 需要收取的费用. 因此, 支付给中间节点的交易费用可以表示为公式(1), 其中, F 代表总的交易费用, F_{base} 代表基础费用, r 代表费率, a 代表流经中间节点的交易金额:

$$F=F_{base}+r\times a \tag{1}$$

在闪电网络中, 每条支付通道(视为无向边)会有两个不同的收费函数, 分别由该边所连的两个节点预先设定. 收费函数的自变量是交易金额, 因变量是交易费用. 这里对收费模型进行简化, 将自变量设定为交易金额而不是转账金额(注: 转账金额是流经中间节点的资金总量, 是交易金额与交易费用之和). 这两个收费函数一般是不同的, 是由两个收费方独立设置的. 由于只有当资金流出一个中间节点时它才会收取费用, 因此, 当

资金沿支付通道某一方向流动时，有且仅有一个收费函数会生效，即资金流出节点的收费函数. 本文中，我们将收费函数表示为包含两个参数(截距和斜率)的线性函数. 截距的实际意义是基础费用，斜率的实际意义是费率. 利用下面的场景来解释收费的具体过程. 如图 1 所示: 对于 Alice 和 Bob 之间的通道 C_i, Alice 将其收费函数设置为 $F_{A_i}=0.03a+0.04$, Bob 将其收费函数设置为 $F_{B_i}=0.02a+0.05$. 这意味着，若交易金额是 6.00 BTC，当资金在通道 C_i 中从 Bob 流向 Alice 时，支付给 Bob 的交易费用为 0.17 BTC; 当资金在通道 C_i 中从 Alice 流向 Bob 时，支付给 Alice 的交易费用为 0.22 BTC.

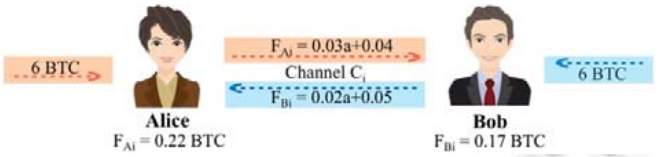


图 1 付款给闪电网络中间节点

2 数据采集与研究方法

自 2018 年 1 月闪电网络在比特币主网发布以来，开通支付通道和关闭支付通道的事务数据都被提交到区块链上，这些数据对公众是开放的. 本文在闪电网络数据统计网站[8]上收集了自其 2018 年 1 月 12 日发布截止到 2020 年 7 月 22 日的这些数据，并进一步加以整理分析. 具体来讲，本文收集了闪电网络支付通道的全面信息，包括节点、通道余额、开通和关闭通道的状态、节点的收费策略等. 通过这些数据，可以分析闪电网络当前的静态拓扑特征、历史特征及其发展趋势.

本文把闪电网络看作是一个无向带权多重图 $G=(V,E)$(多重图指的是在两个节点之间存在多条边的图，需要指出闪电网络中的确存在两个节点之间有多条通道的情况). 其中，V 是节点的集合，E 是边(即支付通道)的集合. 节点 v_i 和节点 v_j 之间的通道表示为 e_{ij}. e_{ij} 的权值为通道的余额. 此外，视情况为节点和边赋予其他相关属性，如节点的收费策略、通道的开闭时间等. 基于收集到的闪电网络数据构建网络图，从多方面深入研究闪电网络的特征.

本文捕获了 2020 年 7 月 22 日闪电网络的快照，用以分析其静态拓扑结构. 基于捕获的快照，本文构建了一个共包含 7 647 个节点、38 659 条边的无向多重图. 选取一些常用于衡量网络特征的属性进行计算，并做出有关解释. 将闪电网络与其他几种典型网络进行对比，观察其共性与差异. 同时，对闪电网络的连通分量及典型特征的分布进行分析. 此外，对闪电网络中节点进行聚类，深入分析节点特征. 为此，本文第 3 节详细介绍了闪电网络的静态拓扑结构.

为了在时间维度上了解闪电网络，以研究其发展趋势，本文自 2018 年 2 月–2020 年 7 月在每月的 1 日对闪电网络摄取一张快照，共计获得 30 张快照. 为每张快照构建网络图，对关乎闪电网络规模和特征的重要指标进行计算，得到其时间序列上的演化过程，进而得以了解闪电网络的发展趋势. 此外，对通道的存在时间及其关闭方式进行研究，从时间维度上细致地了解闪电网络. 上述内容的详细分析见本文第 4 节.

为了进一步明晰闪电网络的收费策略，本文还对链上和链下的交易费用进行了对比. 在衡量链下交易费用时，本文使用了两种路由策略，即费用最小化路由策略和路径长度最小化路由策略. 在这一部分中，将闪电网络视为一个有向图，将一个支付通道视为两条有向边，利用 Dijkstra 最短路径算法构造单路径支付路由，并估算每笔交易的花费. 具体来讲，本实验随机选择收款人和在其通道中有足够余额的付款人，计算两种路由策略下不同交易金额情况下的交易费用和路径长度. 每种情况共进行 500 次支付路由模拟，计算平均交易费用、平均路径长度和交易成功率. 关于收费特征的详细分析见本文第 5 节.

3 闪电网络静态拓扑结构

3.1 基本属性

本文基于 2020 年 7 月 22 日捕获到的闪电网络快照，构建一个共包含 7 647 个节点、38 659 条边的网络.

闪电网络拓扑结构的基本属性见表 1. 网络中的总余额是 1 003.5 BTC. 节点平均度为 10.11. 闪电网络度的同配性为–0.25. 度的同配性是指, 从网络结构的角度考虑节点之间相互连接的可能性. 闪电网络的度同配性为负数, 说明网络中的低度节点更倾向于与高度节点相连, 这意味着闪电网络中可能存在一些较为中心的高度节点.

表 1 闪电网络基本属性

属性	值
节点数	7 647
通道数	38 659
网络总余额(BTC)	1 003.5
网络密度	0.001 3
网络传递性	0.063 7
平均度	10.110 9
平均聚类系数	0.206 8
度的同配性	–0.250 0

图的密度是用来衡量网络稀疏性的, 它被定义为公式(2), 即实际存在边数与可容纳边数上限的比值:

$$D=\frac{2|E|}{|V||V-1|} \tag{2}$$

闪电网络的网络密度是 0.001 3, 说明闪电网络是一个稀疏的网络.

网络传递性表示图中所有现存三角形与潜在三角形的比, 定义为公式(3):

$$T=\frac{3\times number\ of\ trangles}{number\ of\ paths\ of\ length\ 2} \tag{3}$$

闪电网络的传递性是 0.063 7, 这进一步验证了其稀疏性.

局部聚类系数用以衡量一个节点的邻居节点之间的连接程度. 公式(4)定义了节点 u 的局部聚类系数:

$$CC(u)=\frac{2|e_{vw}|}{deg(u)(deg(u)-1)},\ v,w\in N(u),\ e_{vw}\in E \tag{4}$$

其中, $deg(u)$是节点 u 的度数, $N(u)$代表节点 u 邻居节点的集合. 闪电网络的聚类系数较高, 它的平均局部聚类系数为 0.206 8.

为了更好地了解闪电网络的特征, 本文将闪电网络的平均聚类系数、传递性和同配性与相同规模下的典型网络进行对比, 包括规则图、随机图、小世界网络和无标度网络.

规则图是指每个节点都有相同数量的邻居节点(即相同的度)的图. 在随机图中, 每两个节点连接的概率相同, 每条边是否连接相互独立. 小世界网络的特点是节点倾向于聚集且网络密度较高. 无标度网络的特点是绝大多数节点为低度节点, 仅有少部分节点为高度节点. 无标度网络的度分布服从幂律分布, 度为 k 的节点比例为 $P(k)$, 表示为 $P(k)\sim k^{-a}$, 其中, a 的典型范围在 2~3 之间.

如表 2 所示, 闪电网络的平均聚类系数与小世界网络的类似, 比其他网络的大得多. 然而, 闪电网络的网络传递性比小世界网络小得多. 这表明: 尽管闪电网络中的节点倾向于聚集, 但正如前面提到的, 它仍然是一个稀疏的网络. 由于规则图中每个节点的度相同, 则不考虑同配性. 其余 4 种网络均表现出负的同配性, 说明低度节点更倾向于与高度节点相连, 且闪电网络的这种倾向性比其他网络更加突出.

表 2 与同等规模典型网络的对比

	闪电网络	规则图	随机图	小世界网络	无标度网络
平均聚类系数	0.206 8	0.001 0	0.001 2	0.232 4	0.009 6
传递性	0.063 7	0.001 0	0.001 3	0.222 3	0.006 2
同配性	–0.245 0	–	–0.001 3	–0.023 1	–0.036 4

3.2 连通分量

对于子图 $G'=(V',E')$, $V'\subset V$, $E'\subset E$, 如果任何一个节点 $u\in V'$是 V'中其他任何节点都可达的, 则被称作连通分量. 如表 3 所示, 闪电网络由 48 个连通分量组成. 表中的通道平均存在时间指的是从通道开通到捕获快照

时的时间间隔.

表 3 连通分量的一些特征

连通分量		连通分量中的通道	
节点数目	连通分量个数	平均余额(sat)	平均存在时间(天)
7 544	1	2 599 290	341
5	1	200 000	672
3	6	308 923	498
2	40	201 073	495

闪电网络的最大连通分量具有 7 544 个节点和 38 601 个通道, 它的网络直径是 12, 平均最短路径长度为 3.52. 两个节点之间的距离被定义为它们之间的最短路径, 网络直径是指网络中任意两个节点之间距离的最大值. 这个最大连通分量聚集了闪电网络中 98.7%的节点, 在闪电网络中占据主要地位. 关于连通分量的分析表明, 闪电网络实际上是由一个大的中心团簇和一些松散的外围连接组成的.

如表 3 所示, 其余 47 个连通分量均由少量节点组成. 关于仅包含 2 个或 3 个节点的连通分量, 对于它们存在的可能原因, 本文提供以下 3 种猜测.

- 首先, 一些交易双方或者小团体可能会通过闪电网络进行较为频繁的交易. 他们只与对方或者小团体中的其他人进行交易, 所以无需与其他各方相连;
- 其次, 可能存在一些想要尝试闪电网络这一新兴事物的用户, 会自己或与同伴开通一个或两个通道进行实验;
- 此外, 还有一些研究者或许想要进一步研究闪电网络特性并提出相关完善措施, 因此他们形成了小的团队并进行研究.

对于仅有的包含 5 个节点的连通分量, 其通道平均存在时间为 672 天, 远大于其他连通分量. 因此, 它的存在倾向于是上述第 1 种原因. 最大连通分量的通道平均余额远远超过其他连通分量, 这表明其中存在一些中心节点. 但其通道的平均存在时间比其他连通分量都低, 这是由于, 它是闪电网络中最活跃的部分, 有很多新开通的通道都加入了进来.

3.3 典型特征的分布

图 2 展示了闪电网络的度分布情况, 可以看出: 闪电网络中仅有少数高度节点, 大部分为低度节点. 这与先前提到过的无标度网络非常相似. 为了对此进一步加以验证, 采用文献[9]中介绍的方法, 使用极大似然估计来进行幂律拟合. 该度分布的幂律拟合 a 值为 2.11, 因此得到幂律函数为 $y \sim x^{-2.11}$, 度分布的拟合线如图 2 中虚线所示. 此外, 本文使用 Kolmogorov-Smirnov (KS)距离来定义真实数据与幂律拟合之间的差异. 通过最小化 KS 距离, 得到 $x_{\min}$ 值为 19, 进行拟合优度检验后, 得到 p 值为 0.90, 大于 0.10, 因此接受幂律分布假设. 总的来说, 闪电网络度分布服从幂律分布, 表明闪电网络是一种无标度网络.

图 3 展示了局部聚类系数的分布情况, 这表明闪电网络本质上是由一个居优势地位的中心群体和松散连接的外围所组成.

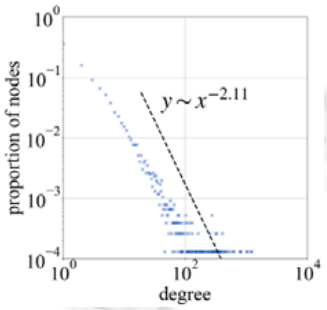


图 2 度分布

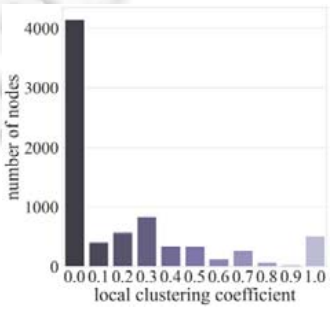
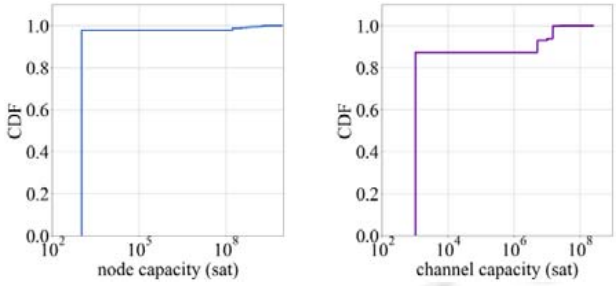


图 3 局部聚类系数分布

图 4 展示了节点余额和通道余额的累积分布函数(cumulative distribution function, CDF). 从图中可以看出, 82.5%的节点和 90.8%的通道余额不超过 10^7 sat (=0.1BTC). 对于余额大于 0.1 BTC 的节点和通道, 我们称之为大型节点和大型通道. 由表 4 可知, 17.5%的节点拥有闪电网络节点总余额的 95.9%, 9.2%的通道拥有闪电网络通道总余额的 59.1%, 这表明, 少数的节点和通道占据了大部分的闪电网络资源.



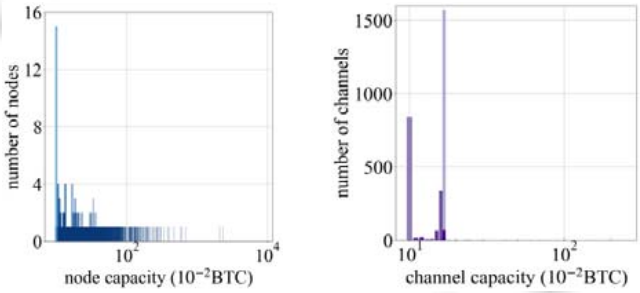
(a) (b)

图 4 节点和通道余额分布

表 4 大型节点和通道

余额大于等于 0.1 BTC	节点	通道
数目	1 341	3570
数目占比(%)	17.5	9.2
余额	1 924.9	582.9
余额占比(%)	95.9	59.1

图 5 展示了大型节点和大型通道余额的分布情况. 大型节点余额的分布集中在 0.1~1.0 BTC, 大型通道余额的分布集中在 0.1~0.2 BTC. 此外, 大型通道的平均存在时间为 278 天, 而全体通道的平均存在时间为 341 天. 这说明, 一些大型通道加入闪电网络的时间相对较晚.



(a) (b)

图 5 大型节点和通道余额分布

3.4 节点聚类分析

为了进一步认识闪电网络中节点的特征和行为, 本文对节点进行了聚类分析. 选取并计算节点的一些属性进行聚类, 包括度、余额、聚类系数、度中心性(degree centrality)、接近中心性(closeness centrality)、中介中心性(betweenness centrality)、特征向量中心性(eigenvector centrality)、基础费用和费率.

网络中节点的重要性可以用节点的中心性来衡量. 度中心性、接近中心性、中介中心性和特征向量中心性是衡量节点中心性的 4 种主要方法. 度中心性是用节点的度来衡量其中心性. 节点 u 的接近中心性被定义为公式(5), 其中, $d(v,u)$是 v 和 u 之间的最短路径距离, n 是可到达 u 的节点数. 接近中心性用来衡量节点与其他节点间的接近程度. 公式(6)定义了节点 v 的中介中心性, 其中, V 是节点的集合, $\sigma(s,t)$是 s 和 t 之间所有的最短路径数, $\sigma(s,t|v)$是 s 和 t 之间所有经过 v 的最短路径数. 中介中心性是节点对网络控制程度的展现. 节点的

特征向量中心性基于其邻居节点的中心性. 与得分高的节点相连, 比与得分低的节点相连对节点分数的贡献要大, 基于此概念, 为网络中的所有节点分配相对分数:

$$C(u)=\frac{n-1}{\sum_{v=1}^{n-1}d(v,u)} \tag{5}$$

$$c_B(v)=\sum_{s,t\in V}\frac{\sigma(s,t|v)}{\sigma(s,t)} \tag{6}$$

本文使用无监督学习的 *K*-Means 聚类算法对闪电网络中节点进行聚类. 通过对聚类效果的评估发现: 当把闪电网络中的节点分为 4 类时, 聚类效果最好. 聚类结果见表 5. 第 1 类包含 7 594 个节点, 占据闪电网络节点数的 99.3%. 该类节点余额较低. 它们的度非常低, 意味着少有邻居节点. 但是该类节点的聚类系数是这 4 类中最高的, 与此同时, 中心性却比其他都低, 说明它们在闪电网络中的重要性比较低. 此外, 第 1 类节点的费率比其他 3 类高很多, 该类中的一些节点可能是为了收取交易费用、赚取资金而建立通道. 第 2 类和第 3 类节点在闪电网络中较为重要, 共计包含 52 个节点, 它们的度、余额、聚类系数、中心性都很高. 显然, 它们就是网络中的中心节点. 与第 2 类节点相比, 第 3 类节点在网络中的重要性更高. 第 2 类节点的基础费用较低, 但费率较高. 第 4 类节点尤为特别, 因为仅包含一个节点. 进一步探索发现, 这个节点是“ACINQ”, 为闪电网络的主要研发公司之一. 从表中可以看出, 它的中心性很高, 是闪电网络中至关重要的节点. 它的度和余额是第 3 类节点的两倍多. 然而它的费率很低, 说明它并不是为了收取交易费而存在的.

表 5 节点聚类结果

类别	度	余额 (BTC)	聚类系数	中心性				基础费用 (sat)	费率	节点数目
				度	接近	中介	特征向量			
第 1 类	7.5	0.12	0.208	0.001	0.282	0.002	0.004	0.875	1.150×10^{-1}	7 594
第 2 类	347.6	17.03	0.112	0.045	0.395	0.015	0.086	0.386	1.184×10^{-3}	46
第 3 类	506.8	36.77	0.061	0.066	0.398	0.022	0.099	1.359	6.028×10^{-4}	6
第 4 类	1 171.0	84.27	0.014	0.153	0.439	0.109	0.135	0.749	7.481×10^{-5}	1

4 闪电网络的发展趋势

4.1 闪电网络的演化

本文从 2018 年 2 月–2020 年 7 月在每月第 1 天捕获闪电网络的快照, 进而获得了闪电网络一些特征的演化趋势.

首先研究闪电网络规模随时间的变化情况. 如图 6 所示, 闪电网络规模呈扩大态势. 节点数稳步增长, 在闪电网络发布初期增长相对较缓, 随后迎来半年多的快速增长时期, 之后便是缓慢增长阶段. 闪电网络通道数与网络总余额的演化趋势较为相似. 它们在 2019 年 1 月–5 月之间增长非常迅速, 之后经历了一段时间的下降, 随后呈现逐渐增长的趋势. 闪电网络的网络密度在开始阶段急剧下降, 之后保持下降趋势.

本文收集了相关资料, 以进一步分析闪电网络经历快速增长期和下降期的原因. 2019 年年初, 一个匿名的比特币用户“hodlonaut”发起了“闪电火炬”活动[10], 吸引了全球近 300 名用户通过闪电网络转移比特币, 其中一些用户在比特币行业非常有名. “闪电火炬”活动使得人们对闪电网络这项技术的发展充满信心. 应用层发展迅速, 钱包数量呈指数型增长. 此外, 一些基础功能(例如瞭望塔[11]和多路径支付)被添加到闪电网络中. 随着闪电网络得到更多的关注, 参与者数目显著增加. 然而在 2019 年 5 月–10 月之间, 网络总余额下降了近 27%. 闪电网络开发者 Russel 表示, 这个下降可能与比特币价格的上涨有关. 或许很多用户认为, 相比于将手中持有的比特币放在一个应用不多的地方, 趁着现有牛市套现更为实际. 值得一提的是, 从 2019 年 11 月开始, 闪电网络重新展现出上升态势, 这可能是由于技术或应用上有了新的突破[12].

根据图 6 所示的闪电网络规模演化趋势, 很容易理解图 7 所示的节点和通道特征的演化趋势. 在演化趋势的后期, 由于通道数的增长程度低于节点数的增长程度, 节点平均度呈下降趋势. 节点和通道平均余额的

演化趋势亦是如此.

节点度分布的演化趋势如图 8 所示. 使用幂律函数 $y\sim x^{-a}$ 拟合闪电网络每月快照的节点度分布, 详细方法参见第 3.3 节. 最终得到了 a 值的变化趋势, 如图 8 所示. a 值越大, 拟合线的斜率越大, 度分布越不均匀, 闪电网络就越加中心化. 从图中可以看出, 闪电网络在中心化趋势和去中心化趋势之间随机波动. 尽管如此, a 值仍处于 2~3 之间, 表明闪电网络的度分布服从幂律分布. 总的来说, 闪电网络的节点度分布类似于无标度网络, 其各节点之间的连接状况(度数)具有严重的不均匀分布性. 网络中存在一些较为关键的重要节点, 所以业界对于其偏离区块链去中心化本质的担忧不无道理.

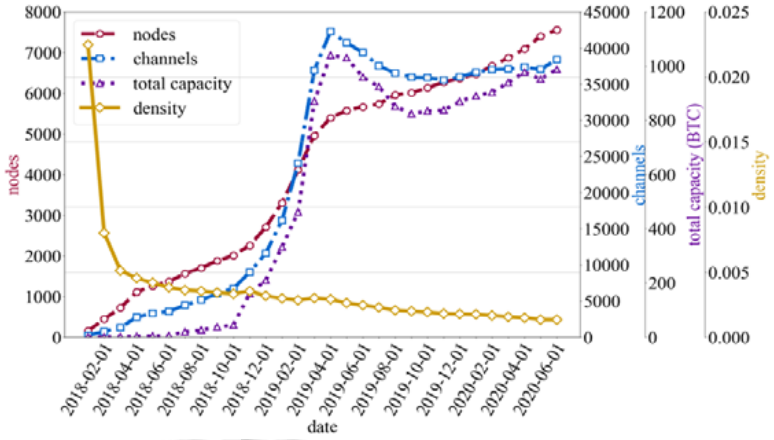


图 6 闪电网络规模发展趋势

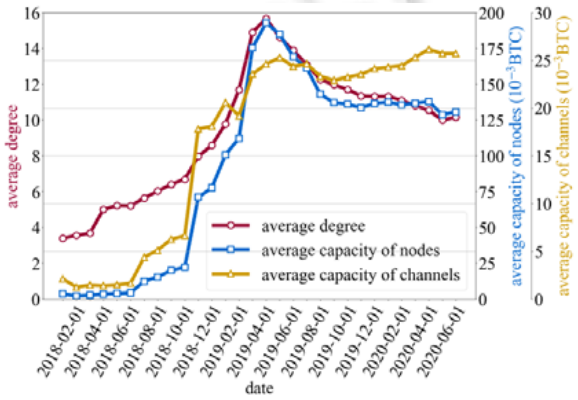


图 7 节点和通道特征发展趋势

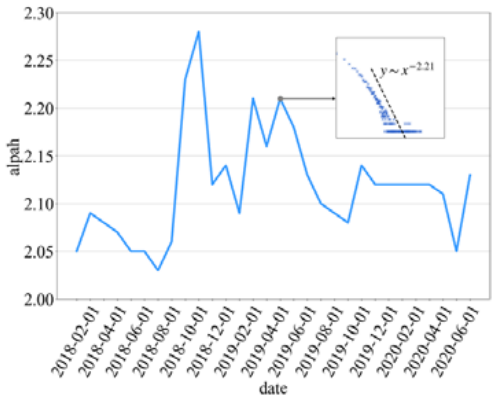
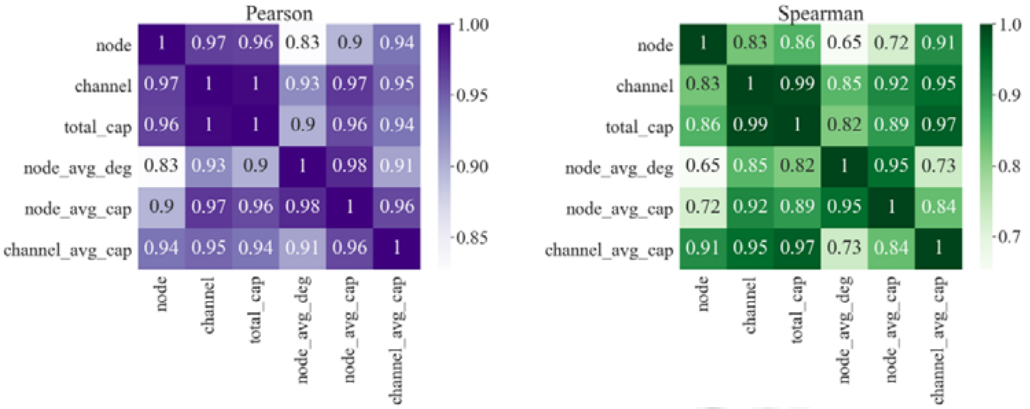


图 8 节点度分布变化趋势

图 9 展现了上述一些特征之间的 Pearson 相关系数和 Spearman 相关系数. 图中的 *node*、*channel*、*total_cap*、*node_avg_deg*、*node_avg_cap*、*channel_avg_cap* 分别代表节点数、通道数、网络总余额、节点平均度、节点平均余额、通道平均余额. Pearson 相关系数是一种线性相关系数, 用于衡量两个变量间的线性相关程度. Spearman 相关系数又称为秩相关系数, 是反映等级相关程度的统计分析指标. 通过观察发现, 这些特征之间的相关性很强. 通道数和网络总余额的 Pearson 相关系数是 1.00, Spearman 的相关系数是 0.99, 可见它们之间的相关性非常强. 节点数和节点平均度之间的相关性是这些关系中相对较弱的, 但它们的 Pearson 相关系数仍达到了 0.83, Spearman 的相关系数为 0.65, 属于强相关关系.

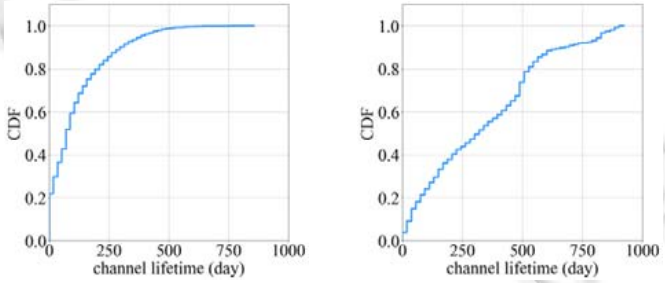


(a) (b)

图 9 相关系数

4.2 通道存在时间

截至 2020 年 7 月 22 日，闪电网络历史开通通道数为 106 159，其中，67 500 条通道已被关闭. 已关闭通道的平均存在时间为 121 天，未关闭通道直至 2020 年 7 月 22 日的平均存在时间为 342 天. 图 10 展示了已关闭通道和未关闭通道存在时间的累积分布函数图. 如图 10(a)所示：超过 20%的已关闭通道存在时间在 1 天以内，近 80%的已关闭通道存在时间不超过 200 天. 由图 10(b)可见：超过半数的未关闭通道已存在时间少于 400 天. 此外，本文还评估了通道存在时间与通道余额的关系. 在所有已关闭通道中，其存在时间与其余额的 Pearson 相关系数和 Spearman 相关系数分别为–0.058 和–0.001 4. 未关闭通道存在时间与其余额间的 Pearson 相关系数和 Spearman 相关系数分别为–0.104 和–0.228. 由于通道数量较大且分布较为分散，本文根据通道存在时间进行分类，并分别对其计算与通道余额之间的关系，见表 6 和表 7.



(a) (b)

图 10 已关闭通道和未关闭通道存在时间分布

表 6 已关闭通道存在时间与通道余额的相关性

通道存在时间(天)	Pearson 系数	Spearman 系数
1–200	–0.032 7	–0.030 3
200–400	–0.018 2	–0.029 8
>400	–0.080 2	–0.107 7

表 7 未关闭通道存在时间与通道余额的相关性

通道存在时间(天)	Pearson 系数	Spearman 系数
<400	–0.056 8	–0.073 9
>400	–0.247 7	–0.469 7

可以看出：在存在时间较久的通道中，特别是在现存通道中，存在时间与通道余额的关系更为强烈，且

呈负相关关系. 一些闪电网络的初始用户可能是为了验证其功能特性, 或者以尝试性的心理, 使用较小的金额开通通道, 而并不是为了满足支付交易的需求.

4.3 通道关闭方式

支付通道的关闭会有不同的方式, 如下给出通道关闭的 3 种方式.

- 第 1 种称为 mutual, 是一种合作的通道关闭方式, 通过广播资金交易的无条件花费并输出给每个对等点来实现;
- 第 2 种称为 force, 是一种不合作的通道单向关闭方式, 通过广播承诺交易实现. 需要指出的是: 关闭时涉及的承诺交易比关闭交易本身规模更大(即效率更低), 且承诺交易中被广播的交易者在事先协商好的一段时间内不能取回在单向关闭的通道内的资金;
- 第 3 种称为 penalty, 是被交易一方恶意撤销交易的支付通道的关闭, 该交易方通过广播想要撤销的交易的承诺交易来实现. 但是由于交易的另一方掌握了承诺交易的密钥, 则前述恶意通道关闭是无效的; 相反, 它还可以创建一个惩罚交易来让恶意撤销交易方损失交易抵押金额.

图 11 展示了已关闭通道的关闭方式. 超过半数的已关闭通道以 mutual 方式被关闭, 以 force 方式被关闭的通道也占了一大部分, 仅有很少一部分通道以 penalty 方式被关闭.

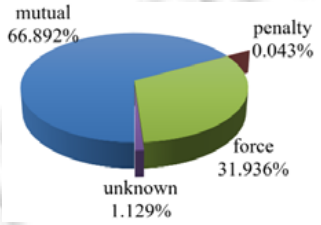


图 11 通道关闭方式

5 闪电网络收费特征

无论是开通支付通道还是关闭支付通道, 都需要缴纳交易费用. 如表 8 所示, 关闭支付通道的费用要高于开通支付通道的费用. 关于基础费用和费率的含义详见第 1.2 节中的解释. 基础费用的中位数和第 90 个百分位数均为 1 sat. 然而, 关于费率的这 3 个值差异很大. 可以看出: 大部分节点的费率设置得非常小; 极少部分节点的费率设置得很大, 这部分节点的存在很可能是为了收取交易费用并获利.

表 8 关于费用的统计

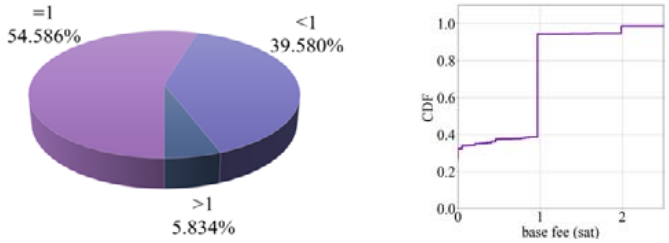
费用的种类	平均值	中位数	第 90 个百分位数
开通通道费用(sat)	5 610.76	2 712	14 181.0
关闭通道费用(sat)	7 472.97	4 423	17 485.2
基础费用(sat)	0.86	1	1
费率	3.24×10^{-2}	1×10^{-6}	1×10^{-3}

下面给出关于基础费用和费率的详细分析.

5.1 关于基础费用的分析

基础费用的分布如图 12 所示: 超过半数的通道将基础费用设置为 1 sat; 仅有 5.834%的通道基础费用设置大于 1 sat, 且大部分将其设为 2 sat.

基础费用与通道余额的关系如图 13 所示, 基础费用的范围取 0–2 sat, 这涵盖了 98.6%的通道. 可以看出: 在在一小部分通道中, 基础费用和通道余额呈线性关系; 但从总体上来看, 这两者之间的 Pearson 相关系数和 Spearman 相关系数分别为 0.008 4 和 0.144 3, 说明基础费用和通道余额间的相关性很弱. 目前, 闪电网络用户对于基础费用的设置体现出一定的随机性和从众性.



(a) (b)

图 12 基础费用的分布

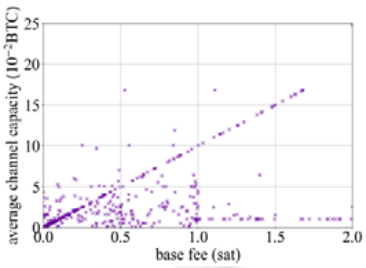
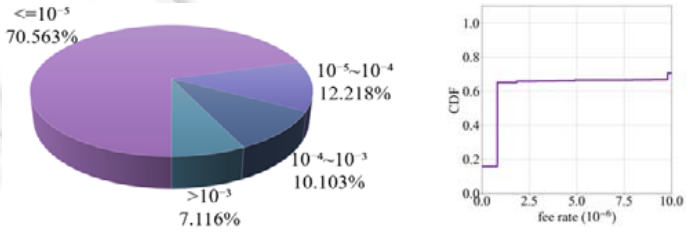


图 13 基础费用与通道余额的关系

5.2 关于费率的分析

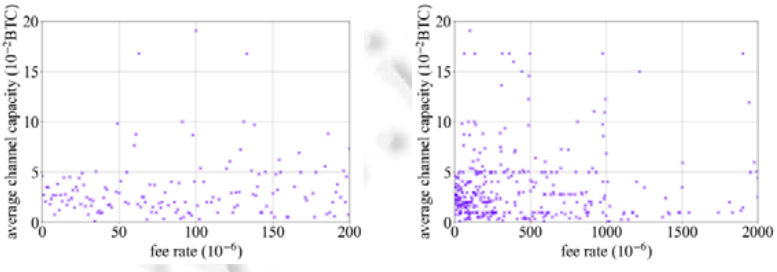
费率的分布如图 14 所示: 超过 70%的通道费率设置低于 1×10^{-5}, 且超过 60%的通道将其设为 1×10^{-6}.



(a) (b)

图 14 费率的分布

费率与通道余额的关系如图 15 所示. 在图 15(a)中, 费率的范围取 0–2×10^{-4}, 这涵盖了 83.6%的通道. 图 15(b)的费率范围取 0–2×10^{-3}, 涵盖了 95%的通道. 费率和通道余额之间的 Pearson 相关系数和 Spearman 相关系数分别为–0.002 2 和 0.289 1, 说明两者有一定非线性的正相关性, 但相关性较弱.



(a) (b)

图 15 费率与通道余额的关系

5.3 链上与链下交易费用的比较

为了深入了解交易通道网络收费的特点, 本节比较了链上和链下的交易费用. 具体方法在第 2 节中有所提及. 由于链上交易费用与许多因素相关且难以通过实验的方式获取到交易费用, 所以这里使用开通通道交易和关闭通道交易作为链上交易的代表. 本文通过计算开通通道和关闭通道的平均费用, 得到链上交易的平均费用, 为 6 334.59 sat.

(1) 费用最小化

这里我们考虑费用最小化策略来进行路由支付, 结果见表 9. 随着交易金额的增大, 平均交易费用有一种粗略的成倍增大的趋势. 随着交易金额的增大, 能覆盖交易费用的可用通道数减少, 交易成功率会下降. 将链下和链上的平均交易费进行对比后发现: 链下交易比链上交易费用低得多, 即使当交易金额达到0.01 BTC时, 链下交易的平均费用也仅为 664.049 sat, 比链上交易费用(6 334.59 sat)低了一个数量级. 进一步探究可知: 对于余额大于 0.01 BTC 的通道, 其平均基础费用为 0.895 sat, 平均费率为 6.103×10^{-3}, 结合上文对费率分布的分析, 能够覆盖 0.01 BTC 的通道相对来说费率较高.

表 9 链下交易费用(费用最小化)

交易金额(sat)	平均费用(sat)	平均路径长度	成功率(%)
10 000	2.862	7.80	86.4
100 000	29.781	7.44	53.8
500 000	225.211	6.10	26.2
1 000 000	664.049	6.06	23.3

(2) 路径长度最小化

这里我们考虑路径长度最小化策略来进行路由支付, 结果见表 10. 随着交易金额的增大, 平均交易费用显然比费用最小化策略增长得更明显. 成功率的数值及其变化趋势与费用最小化策略中的结果相似. 由表 10 可知: 在此种交易策略下, 当交易金额小于 500 000 sat 时, 链下的平均交易费用远低于链上. 然而, 当交易金额增大到 1 000 000 sat时, 由于可用于路由的通道数减少, 则平均交易费用急剧增大, 甚至高于链上的平均交易费用.

表 10 链下交易费用(路径长度最小化)

交易金额(sat)	平均费用(sat)	平均路径长度	成功率(%)
10 000	14.53	5.00	87.0
100 000	121.56	4.73	51.2
500 000	753.65	4.51	23.4
1 000 000	11 606.61	4.37	20.0

除此之外, 无论是费用最小化策略还是路径长度最小化策略, 随着交易金额的增大, 平均路径长度都在减小. 这可能是因为那些余额相对较大的通道具有一定的聚集特征. 在闪电网络的最大连通分量中, 对所连通道中余额大于 0.1 BTC 的节点, 计算其平均最短路径长度, 得到的数值为 1.59. 最大连通分量中所有节点的平均最短路径长度为 3.52. 这个结果基本证实了上述观点.

6 相关工作

据调研, 从拓扑学角度研究网络的方法已经较为成熟, 这些方法同样适用于闪电网络的研究. 本文首先从网络图分析的一般方法中得到一些启发, 然后重点关注比特币系统和闪电网络的图分析.

6.1 网络图分析的一般方法

在网络图分析中, 有很多用于评估特殊属性的方法. 网络的扩展性可以通过多种方式进行研究. S-metric 最先由 LunLi 等人在文献[13]中提出, 用于评估网络无标度的程度. 利用文献[9]中提到的方法, 基于实验数据可以证明网络的无标度性. 聚类系数和相关系数也是网络分析中的重要参数. 本文应用了文献[14–17]中的部分理论来解释数据含义. 此外, 中心性也是去中心化网络研究中较为重要的因素. 从文献[18–20]中得到启发, 本文采用了更好的方法来研究网络的内聚子群结构.

6.2 比特币系统的图分析

近来的一些工作[21−27]细致研究了比特币的点对点覆盖. 一些文献[22−24]专注于研究和改进信息传播及其延迟. Miller 等人[21]对于比特币网络的公共拓扑进行了调查, 并发现了一些有影响力的节点. 比特币交易图也吸引了众多研究者的关注[25−27]. 例如, DoritRon[26]对与比特币交易策略相关的交易图的统计特性进行了定量分析, 发现了用户的典型行为和隐私保护的方法. 本文采用 Reid 等人[28]的方法将闪电网络抽象为一个无向带权图, 其中每个节点代表一个参与者, 边代表支付通道, 其权值代表该通道中的余额.

6.3 闪电网络的图分析

虽然闪电网络只投入使用不到 3 年, 但对它的研究有很多[2−7]. Martinazzi 等人在文献[3]中研究了闪电网络的拓扑特征变化及其效率和同步性. 此外, 一些研究者在拓扑研究的基础上, 对安全问题也进行了探讨. 例如, 文献[4]分析了闪电网络对基于拓扑的攻击的恢复能力. 除了上述几个方面外, 闪电网络的路由问题也是研究的热门问题. Flare[5]是当前闪电网络的路由方法, 它的优点是寻找路径时效率很高. 当然还有许多其他具有不同优势的路由策略, 例如文献[6]中的多路径路由支付方案, 大大降低了交易费用. 此外, 还有一些对闪电网络中的交易所进行的模拟研究. Béres 等人[7]为闪电网络设计了一个用于分析不同节点的路由成本和潜在收益的流量模拟器. 本文利用收集到的数据构建网络图进行全面的统计计算, 在此基础上给出了详实的解释和合理的推测. 此外, 本文还重点研究了闪电网络的收费机制, 通过进行交易仿真, 以对比闪电网络和比特币链上的交易费用.

7 结 论

本文基于具有高时效性的大量数据, 运用典型图分析方法对闪电网络进行研究, 对闪电网络中节点和通道的静态和动态拓扑特征进行了全面的分析. 利用上述静态和动态度量, 在闪电网络中进行节点聚类, 并根据聚类结果得到全面的结论和合理的推测. 全面研究了闪电网络的规模发展趋势、节点和通道特征以及节点的度分布等. 此外, 本文还特别对闪电网络的收费特征进行了详尽的研究. 通过在闪电网络中模拟费用最小化和路径长度最小化两种路由策略, 得到链下交易费用的估计; 通过进行合理的近似假设, 得到链上交易费用的统计; 最后, 通过两种交易费用的比较, 直观地证明了闪电网络出众的应用价值.

References:

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

[2] Seres IA, Gulyás L, Nagy DA, Burcsi P. Topological analysis of bitcoin’s lightning network. arXiv preprint arXiv: 1901.04972, 2019.

[3] Martinazzi S, Flori A. The evolving topology of the lightning network: Centralization, efficiency, robustness, synchronization, and anonymity. PloS One, 2020, 15(1): e0225966.

[4] Rohrer E, Malliaris J, Tschorsch F. Discharged payment channels: Quantifying the lightning network’s resilience to topology-based attacks. In: Proc. of the IEEE European Symp. on Security and Privacy Workshops (EuroS&PW). IEEE, 2019. 347−356.

[5] Prihodko P, Zhigulin S, Sahno M, Ostrovskiy A, Osuntokun O. Flare: An Approach to Routing in Lightning Network. White Paper, 2016.

[6] Di Stasi G, Avallone S, Canonico R, Ventre G. Routing payments on the lightning network. In: Proc. of the IEEE Int’l Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018. 1161−1170.

[7] Béres F, Seres IA, Benczúr AA. A cryptoeconomic traffic analysis of bitcoins lightning network. arXiv preprint arXiv: 1911.09432, 2019.

[8] LNchannels. https://ln.bigsun.xyz/

[9] Clauset A, Shalizi CR, Newman MEJ. Power-law distributions in empirical data. In: Proc. of the SIAM Review. 2019. 661−703.

[10] Bitcoin's 'lightning torch' explained. https://www.coindesk.com/bitcoins-lightning-torch-has-blazed-through-37-countries-so-far

[11] Watchtowers. https://www.coindesk.com/blockstreams-watchtowers-will-bring-a-new-justice-system-to-the-lightning-network

[12] Bitcoinnews. https://www.coindesk.com/a-dangerous-bug-in-bitcoins-lightning-network-has-been-fixed

[13] Li L, Alderson D, Doyle JC, Willinger W. Towards a theory of scale-free graphs: Definition, properties, and implications. Internet Mathematics, 2005, 2(4): 431−523.

[14] Just W, Callender H, LaMar MD. Clustering coefficients. Technical Report, Dosegljivo: Ohio University, 2015. https://qubeshub.org/resources/741/download/ModuleCCQ.pdf

[15] Lee J, Rodgers W, Nicewander A. Thirteen ways to look at the correlation coefficient. The American Statistician, 1988, 42(1): 59−66.

[16] Taylor R. Interpretation of the correlation coefficient: A basic review. Journal of Diagnostic Medical Sonography, 1990, 6(1): 35−39.

[17] Saramäki J, Kivelä M, Onnela JP, Kaski K, Kertesz J. Generalizations of the clustering coefficient to weighted complex networks. Physical Review E, 2007, 75(2): 027105.

[18] Estrada E, Rodriguez-Velazquez JA. Subgraph centrality in complex networks. Physical Review E, 2005, 71(5): 056103.

[19] Brandes U. A faster algorithm for betweenness centrality. Journal of Mathematical Sociology, 2001, 25(2): 163−177.

[20] Borgatti SP, Everett MG. A graph-theoretic perspective on centrality. Social Networks, 2006, 28(4): 466−484.

[21] Miller A, Litton J, Pachulski A, Gupta N, Levin D, Spring N, Bhattacharjee B. Discovering bitcoin's public topology and influential nodes. 2015. https://allquantor.at/blockchainbib/pdf/miller2015topology.pdf

[22] Neudecker T, Andelfinger P, Hartenstein H. Timing analysis for inferring the topology of the bitcoin peer-to-peer network. In: Proc. of the Int'l IEEE Conf. on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and SmartWorld Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld). IEEE, 2016. 358−367.

[23] Decker C, Wattenhofer R. Information propagation in the bitcoin network. In: Proc. of the IEEE P2P 2013. IEEE, 2013. 1−10.

[24] Fadhil M, Owenson G, Adda M. A bitcoin model for evaluation of clustering to improve propagation delay in Bitcoin network. In: Proc. of the IEEE Int'l Conf. on Computational Science and Engineering (CSE) and IEEE Int'l Conf. on Embedded and Ubiquitous Computing (EUC) and the 15th Int'l Symp. on Distributed Computing and Applications for Business Engineering (DCABES). 2016. 468−475.

[25] Ober M, Katzenbeisser S, Hamacher K. Structure and anonymity of the bitcoin transaction graph. Future Internet, 2013, 5(2): 237−250.

[26] Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Springer, 2013. 6−24.

[27] Fleder M, Kester MS, Pillai S. Bitcoin transaction graph analysis. arXiv preprint arXiv: 1502.01657, 2015.

[28] Reid F, Harrigan M. An analysis of anonymity in the bitcoin system. In: Proc. of the 3rd IEEE Int'l Conf. on Privacy, Security, Risk and Trust (PASSAT)/the 3rd IEEE Int'l Conf. on Social Computing (SocialCom). IEEE, 2011. 1318−1326.

陈艳姣(1989－), 女, 博士, 研究员, 博士生导师, 主要研究领域为无线网络安全, 区块链.

于永瑞(1999－), 女, 博士生, 主要研究领域为计算机网络, 区块链.

朱笑天(1996－), 女, 博士生, 主要研究领域为计算机网络, 区块链.

程子英(1999－), 女, 博士生, 主要研究领域为计算机网络, 区块链.