基于区块链的支付信道网络：挑战与发展

徐秀[1]，田安琪[2]，何瑞雯[2]
（1.中国信息通信研究院，北京 100083；2.中国科学院软件研究所，北京 100190）

摘　要：与传统金融系统的事务负载相比，区块链的事务处理能力并不占优势。支付信道是目前提高区块链系统性能的主流研究方向之一，其功能包括降低交易确认时延和提高系统交易吞吐量。支付信道网络允许大量交易离链执行，可在保证资产安全的同时降低费用并促进区块链规模化。作为支付信道网络最知名的工作，闪电网络部署在比特币之上，其在实际运行中展现了高效的性能和高昂的经济效益，引发了大量关注与研究。对以闪电网络为代表的支付信道网络研究工作进行系统化梳理，整理分析闪电网络的潜在攻击和改进方向。在此基础上，将现有研究成果细化到安全性攻击、隐私漏洞和难以实现的系统假设等方面，针对闪电网络的关键挑战进行详细调研，并比较现有解决方案。最后，突出了支付信道网络的发展潜力，并确定了亟待解决的关键问题，以推进区块链支付信道网络的研究。

关键词：区块链；低时延；高性能；支付信道网络；闪电网络
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024217

Blockchain-based payment channel network: challenges and recent advances

XU Xiu[1], TIAN Anqi[2], HE Ruiwen[2]
1. China Academy of Information and Communications Technology, Beijing 100083, China
2. Institute of Software, Chinese Academy of Sciences, Beijing 100190, China

Abstract: The transaction processing speed of blockchains is not superior to that of the traditional financial system. Payment channel is one of the mainstream research directions to improve the performance of blockchain systems, and its functions include reducing transaction confirmation delay and increasing system transaction throughput. Payment channel networks allow a large number of transactions to be executed off-chain, which can reduce costs and facilitate blockchain scaling while keeping assets secure. As the most well-known work on payment channel networks, the Lightning Network is deployed on Bitcoin, and its demonstration of efficient performance and high economic benefits in practical operation has triggered a great deal of attention and research. This thesis systematizes the research work on payment channel networks represented by the Lightning Network, organize and analyze the potential attacks and improvement directions of the Lightning Network. Based on this, this thesis refines the existing research results into security attacks, privacy vulnerabilities and difficult-to-implement system assumptions, conducts detailed research on the key challenges of the lightning network, and compares the existing solutions. Finally, this thesis highlights the development potential of payment channel networks and identifies key issues that need to be addressed in order to advance the research on blockchain payment channel networks.

Keywords: blockchain, low-latency, high-performance, payment channel network, lightning network

0　引言

区块链的诞生[1]和以比特币为代表的数字加密货币的日益普及，使区块链技术受到了空前的关注，并成为一种全新的去中心化基础架构与分布式

收稿日期：2024–10–08

计算范式。由此，引发了人们对基于区块链构建新型数字货币系统以及区块链理论与方法的深入研究。区块链技术是不可信网络环境中一种由多方共同维护的记账技术，它提供了一种开放环境下不依赖任何可信第三方的新型信任建立模式，由相互独立的参与方共同维护系统运行，实现了不可信环境下的信任建立。区块链上复杂的交易逻辑可以借助智能合约得到支持。

然而，随着区块链技术被高度重视与深入研究，其在性能方面的问题日益突出，这制约了区块链技术的实际有效应用。其中，区块链共识协议的性能有2个衡量指标：系统交易处理量和交易确认时间。区块链上的交易处理速度限制在大约每秒10笔交易[2]，确认一个交易需要大约一小时，远低于Visa等传统金融托管系统提供的每秒数千笔交易的处理速度。因此，这种巨大的性能差异使目前的区块链技术无法支持实际应用中海量业务并发与高频交易的需求，限制了其大规模应用。

目前实现高性能区块链系统的解决方案有修改区块链共识架构、分叉和侧链等[3]，其中一些工作已有系统化的整理[4-5]。然而，修改共识机制等方案意味着在现有实际使用的区块链系统上进行改变，如新系统缺乏向后兼容性，这显然将阻碍以上方案在现有区块链上的部署实施。此外，共识机制的改变甚至可能导致严重的系统漏洞和未知攻击的引入。

支付信道已成为提高区块链性能的一种新的解决方案[6]。支付信道允许任意2个用户将资金存入双方共同控制的公共账户，并在链下执行多次两方间的支付，其中仅有建立和关闭信道的交易事务需在区块链上公布。而当协议执行失败时，用户可撤回锁定在两方账户中的资金。由于支付交易的有效性仅由双方链下验证，不需要等待全网诚实节点的确认，其确认时延仅与通信带宽和时延相关，因此降低了交易确认时延；进一步地，由于用户间的多次交易中仅有两笔需被提交并得到全网诚实节点的确认，系统交易吞吐量因此得到了显著提高。多跳支付协议将支付信道扩展到网络，即支付信道网络。它为没有直接链接的任意2个用户提供了支付信道，由中间节点协助完成交易。由于该技术借助其他中间用户作为支付中继建立任意2个用户间的支付路径，故用户间不必彼此建立信道（如锁定一定额度的资产），从而降低了维护信道的成本。例如，闪电网络（LN）就是一个部署在比特币上的实用支付信道网络[7]，该方案自提出以来不断扩张，截至目前已托管价值超过1.7亿美元的比特币，成为支付信道网络方案优越性的可靠证明。

基于区块链支付信道网络领域的快速发展，本文注意到，目前缺乏对相关研究成果实时且成体系的整理。因此，本文的目标是对支付信道网络现有的工作进行整合评估，提供近期支付信道网络研究领域代表性成果的系统概述，为同领域研究者提供一个简明的参考，并为未来的工作提供指导。

1 相关知识

1.1 区块链

区块链是一个仅支持追加的分布式交易账本，用于记录网络中各个节点提交的事务，以便公开验证[8]。用户公布的每笔交易都将记录在区块链的一个数据块上，此即区块链状态的一次不可篡改的更新。链上各方可以通过交易事务交换数字资产，区块链将维护用户的账户余额。根据用户加入条件不同，可以将区块链分类为公有链、私有链和联盟链。

区块链的2个基本属性是一致性和活性。一致性指任意2个诚实节点持有的本地最优链相同；活性指有效事务会在一定时间内被添加到分类账中。共识协议是区块链技术的核心，它规定了分布式场景下，节点间实现本地数据一致存储和状态转变的策略，对区块链系统的安全运行及实际有效应用起决定作用。主流区块链共识算法依赖于计算代价高昂的工作证明（POW）[9]或权益证明（POS）。比特币的区块链基于受限的脚本语言，使用未花费交易（UTXO）形式记录交易，而以太坊等其他区块链基于图灵完备语言，支持高度表达的智能合约[10]。其中，智能合约是指在区块链上执行的一段代码，负责接收硬币，并在用户或其他合约触发时按照预定义的规则进行处理。此外，也存在以Monero为代表的区块链不依赖任何脚本，被称为无脚本区块链。

1.2 链上事务ACID

ACID是数据库数据管理的4个基本属性：原子性、一致性、隔离性、持久性，其目标是保障数据库的可靠性和一致性[11]。由于区块链分布式账

本的性质，区块链上的事务是系统状态的一个实例，同样具备ACID的属性，即：1) 一个事务或由多个事务组成的事务块，要么作为一个整体执行，要么不执行；2) 每笔交易都将区块链系统从一个一致有效的状态转换为另一个，而不损害任何验证规则和数据完整性限制；3) 同时进行的交易安全、独立地执行，不受到其他交易的影响；4) 一旦事务成功公布并记录到链上，则由它产生的所有更改也成为永久的。在区块链协议设计中，保证事务的ACID属性非常重要，否则将导致区块链的安全性出现极大漏洞。

1.3　支付信道

支付信道支持离链单向支付，且可以在此基础上过渡到双向信道设计。在双向支付信道中，交易双方都可以支付或收款，其核心思想是允许双方多次商定信道内资金分配状态，最终将一致同意的分配状态公布到区块链上。信道生命周期由3个阶段组成，即信道建立、信道更新和信道关闭或纠纷。其中信道更新过程如图1所示。

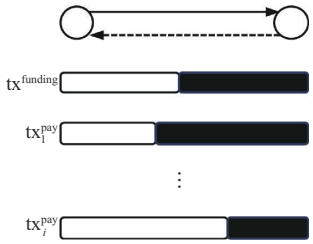

图1　信道更新过程

信道建立阶段，双方通过公布交易事务上链，将一部分资金存入共同控制的多重签名地址中，存入的资金总和称为信道容量；信道更新阶段，双方通过调整信道容量的资金分配状态完成支付；在信道关闭或纠纷阶段，双方将最新的资金分配状态公布上链，被锁定的资金按照该分配方案，从多重签名账户回到双方账户，从而完成信道关闭。

1.4　支付信道网络

支付信道网络（PCN）是由支付信道组成的网络，用于在没有建立直接支付信道的2个用户之间执行离链支付。其原理即由其他用户作为中介，利用已建立的支付信道形成支付路径。PCN可以表示为一个有向图$G=(V, E)$，其中顶点集V代表用户，加权边集E代表支付信道。每个顶点$U\in V$都关联一个非负数，该非负数表示它为转发支付而收取的费用。如图2所示，用户A和E没有建立直接的支付信道，但可以通过连接它们的多跳路径进行支付，即A可以向B进行支付，B在此过程中收取中介费用，继续向C支付，C收取中介费用，继续向D支付，以此类推。最终，A通过A→B→C→D→E的路径向E完成支付，而B、C、D在该路径中作为中介节点传递交易，并收取相应费用。这里忽略了保证多跳支付安全性的机制，只对支付路径本身进行演示，当路径沿线的所有用户都有足够的余额时，就可以完成支付。

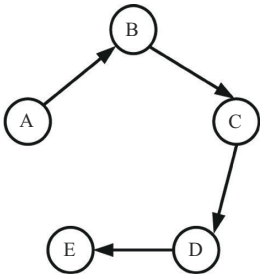

图2　PCN多跳支付示意

2　闪电网络

闪电网络部署在比特币上，是支付信道网络最具代表性的例子。它由Poon和Dryja在2015年的白皮书中提出[7]，闪电网络核心架构如下。

1) 序列到期可撤销合约（RSMC, revocable sequence maturity contract）部署在两方支付信道上，以保证支付信道内链下交易的正确进行和记录。合约由信道建立、更新、关闭3个阶段组成。

在信道建立阶段，双方拟定一条抵押交易$tx^{funding}$，用于将一部分资金转移到由双方共同控制的公共地址中。双方完成确认后，开始分别构建承诺交易$tx^{commitment}$，并再分别构建指向承诺交易的退款交易tx^{refund}，其中tx^{refund}将在$tx^{commitment}$合法后的一段时间后合法。交易$tx^{commitment}$和交易tx^{refund}均指向事务$tx^{funding}$，在事务$tx^{funding}$发布在链上前，前述交易均不合法。随后，双方互换构建的承诺交易$tx^{commitment}$和退款交易tx^{refund}，并且为对方的交易签名。当双方都收到对方签名的交易并确认无误后，即可在抵押交易$tx^{funding}$上签名并上链，完成支付信道的建立。

在更新阶段，在第i次交易之前，双方将tx_{i-1}^{refund}的输入地址对应的私钥$sk_{i-1}^{M}, M\in\{A,B\}$发送给对方。双方确认收到后，分别构建$tx_i^{commitment}$和

tx_i^{refund}交易，随后互换交易并为对方交易签名。

在关闭阶段，双方中的一方将最新的交易$tx_i^{commitment}$和交易tx_i^{refund}公布到链上，在2个交易都合法后，即可合法地关闭支付信道。

在关闭阶段中，如果另一方在链上观测到负责关闭信道的一方作弊，即将旧交易$tx_x^{commitment}$和$tx_x^{refund}, 0 < x < i$在链上公布，在tx_x^{refund}合法前的等待时间里，可以使用作弊方该次交易输入地址对应的私钥sk_x构建交易并公布上链，取走作弊方在该地址内的所有资金。该惩罚机制确保了在敌手作弊的情况下，诚实方将永远获得不少于自身应得的财产，同时敌手也将获得一定的惩罚，减少其作弊的动机。

2) 哈希时间锁合约（HTLC, hashed timelock contract）通过区块链的时间锁脚本，保证在多个节点之间原子有序地完成交易。其核心原理为：双方约定转账方先冻结一部分资金，即发送比特币到一个由多重签名地址，并由最终接收方生成的一个原像k的哈希值$H(k)$加锁。如果在一定时间内接收方知晓了原像k，使它的哈希值$H(k)$和锁定条件值相同，则这部分资金转给接收方。如果约定时间内，接收方未知晓原像k，则转账方可取回已冻结资金。合约在流程上主要由锁定和解锁两阶段构成，如图3所示。

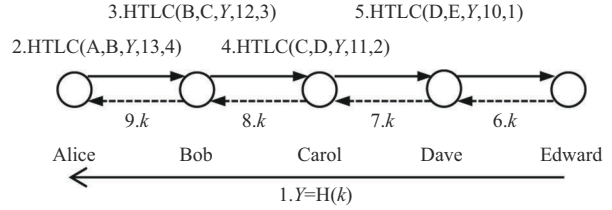

图3 基于HTLC的多跳支付示意

在锁定阶段，接收方Edward生成原像k并将其哈希值Y发送给发送方Alice，Alice以此为锁定条件构建HTLC合约，将一部分资金冻结到Alice与Bob的多重签名地址，路径上的其他节点依次构建HTLC合约和锁定资金，直到接收方Edward确认支付路径已经建立完成。

在解锁阶段，由接收方Edward首先提供原像k解锁并提取Dave冻结的资金，路径上的中介节点以此以原像k提取前一个节点冻结的资金并获得一笔费用，直到发送方Alice冻结的资金被顺利解锁提取，即完成了一次多跳支付。

2.1 安全分析

闪电网络的概念提出后，其安全性备受关注。文献[12-13]对其安全性进行了完备的分析和证明。目前针对闪电网络的攻击主要有2种。

2.1.1 虫洞攻击

虫洞攻击由Malavolta和Moreno-Sanchez在2018年提出[14]，指2个串通的恶意节点在两阶段提交协议的解锁阶段合谋，通过另外的通信信道直接传递哈希原像，跳过2个节点之间的诚实节点，从而非法获取本应由这些诚实节点收取的中介费用。当虫洞攻击发生时，支付过程将无法满足原子性。对于2个恶意节点区间之外的节点，支付正常进行；而被恶意节点包围的节点则会收到恶意节点的交易状态回滚消息，从而支付失败。

此外，虫洞攻击也将降低支付信道网络流动性。在锁定阶段，被窃取费用的诚实节点冻结了一部分资金，但由于它在解锁阶段被恶意跳过，故这一部分资金无法被解锁并用于其他交易。虫洞攻击原理如图4所示。

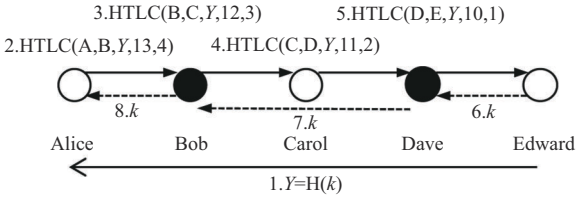

图4 虫洞攻击原理

2.1.2 悲伤攻击

悲伤攻击[15]指敌手向节点发送大量无效请求，以阻塞诚实节点的有效请求。这在支付信道网络中体现为：恶意用户启动链下多跳支付，随后拒绝服务使支付失败，引起诚实用户锁定其资金，从而降低支付网络的总体吞吐量。假设在支付路径存在n个节点，则恶意节点可以利用相对较少的α硬币，锁定该条路径上的$(n-1)\alpha$硬币，在较低成本的前提下使支付信道网络的活性大大降低。

其具体攻击过程如下。1) 选择合适的攻击路径。2) 攻击者通过该路径向另一个攻击者进行多次小额交易，达到最大并发HTLC合约数量，并延迟付款的执行，从而将该路径锁定。3) 在HTLC合约时间到期之前，攻击者主动发布交易失败信号，避免通道被迫关闭，随后再进行下一轮攻击。

2.2　隐私分析

以闪电网络为代表的支付信道网络为增进区块链的性能和隐私性提供了良好的解决方案。但目前针对闪电网络相关的研究主要集中在可扩展性、通用性和安全性上，对其隐私性的研究较少。闪电网络的隐私性包括：信道隐私、第三方余额隐私、中间关系匿名和路径外支付隐私，即 2 个节点之间的信道交易和余额均对外保密，仅有信道容量和参与方公开，在支付路径上的节点仅知道邻居节点的信息，支付路径以外的节点无法推断得知多跳支付的支付值和参与节点。文献[16]对闪电网络的隐私性在模拟运行环境下分别进行了攻击，实验结果并不符合闪电网络的隐私性预期，表明闪电网络在隐私性上仍然存在易于攻击的缺陷，这也将以闪电网络为代表的支付信道网络协议设计的隐私性问题带入大众视野。

3　现有问题及解决方案

虽然现有的以闪电网络为代表的支付信道网络有效提升了区块链的系统性能，但仍存在一定缺陷，如安全攻击（如虫洞攻击和悲伤攻击）、隐私漏洞（如链接性攻击）和难以实现的系统假设（如节点经常在线）等，这些缺陷成为支付信道网络领域的研究热点。本节将针对闪电网络存在的关键问题，重点讨论现有解决方案并给出可能的研究方向。

3.1　通用性

目前，包括闪电网络在内的主流支付信道网络均构建在有底层脚本的区块链上。对区块链的脚本要求导致其通用性受到了一定限制。然而以 Monero 和 ZCash 为代表的无脚本区块链在市场中同样占据了不容小觑的份额，其中 Monero 的市值超过 25 亿美元，ZCash 的市值超过 12 亿美元。如何在无脚本区块链上实现性能良好的支付信道网络，同样成为公开的挑战。

无脚本区块链缺乏时间锁定脚本，因此需另行设计可撤回的资金锁定功能。目前相关领域的工作主要有以下 2 个方向。1) 利用一定规模的困难问题计算时间代替锁定时间。例如文献[17]中提出的属性可验证的定时承诺（AVTC, attribute verifiable timed commitment），其核心思想是由接收方提供给支付方一个线性计算的困难问题，该困难问题的解可被支付方用于构建撤回资金的交易，从而保证诚实方在一定时间后可撤回锁定资产。但该方案需要消耗一定计算资源，且形成的支付信道存在生命周期，目前并未看到该研究方向的工作有进一步的进展。2) 利用适配器签名保证交易的原子性。文献[18-19]均提出了类似的支付信道设计，利用可以连续生成的适配器签名进行链下交易，交易双方在发生纠纷时向可信第三方求助关闭信道。并且，文献[19]以此为基础构建了支付信道网络 Monet，整体工作较为完善。但可信第三方的假设在实际环境中难以满足，如何进一步弱化可信第三方的假设将成为该研究方向接下来的工作主题。

3.2　可靠性

由于支付信道网络中的多跳支付需要跨越多个节点，整条路径的支付成功与否便与路径上的节点状态息息相关。例如，在闪电网络实际运行环境中，若中间节点支付失败，则整条路径的支付也将失败，路径上所有节点需等待资产冻结时间到期退回后重新启动支付，从而在支付过程中消耗大量时间资源。支付失败的原因除路径因意外关闭外，也存在中间节点资源利用不当、资金失衡或耗尽等因素。不仅如此，路径越长，付款方将支付越多的费用给中间节点，导致支付操作更昂贵，因此支付的可靠性也成为支付信道网络设计的考虑因素之一。

文献[20]中提出了兼容以比特币为代表的 UTXO 模型货币的虚拟信道设计，该设计可以直接应用于闪电网络以降低其时延和成本。其核心思想是，将中间节点抽象为一个中介，它在常规交易流程中不需要介入，仅在交易完成时协同参与信道的关闭过程，以此降低中介对支付本身的影响。除此之外，其对惩罚机制的设计保证了旧交易被发布到链上时，诚实一方可以获得虚拟信道中的所有资金，而诚实中介将不受影响；文献[21]则提供了一种支付信道网络的改良方案，称为实践支付信道网络（PPCN）。该方案在网络中引入平衡性与可靠性更好的超级节点（通常为供应商），并通过路由算法将交易路径尽量分配至此类节点上，而非普通的客户节点上，提高交易路径稳定性。

对于路由算法导致的流动性不均匀与路径过长等问题，目前也已有相关优化方案出现。一种常见的思路是将支付信道网络采用的源路由算法改为分

布式路由算法，如文献[22]中提出一种去中心化路由算法Swift，利用秘密路径的设计缩短交易路径长度，优化交易费用与吞吐量，从而增强支付信道网络整体流动性。

3.3 再平衡问题

在支付信道网络中，已建立支付信道的双方均在信道内锁定了一定数额的资产。然而，由于信道两方向的支付流量存在不均衡，资金会逐渐向流量较高的方向累积。这一过程最终将导致信道内的资金完全归属于其中一方，即出现流动资金枯竭的局面，使支付仅能单向进行。这一状况进而削弱了支付信道网络的整体吞吐量。

针对如何让信道双方资金重新趋于平衡，即再平衡问题，目前有以下解决思路。1) 关闭现有支付信道并重新建立。这一操作将带来2个代价高昂的链上事务，针对这一问题，闪电网络开发团队提出了LOOP，将关闭和新建信道成本降低至一个链上事务。但由于平衡后的信道仍可能陷入枯竭，因此可能需要执行多次平衡操作，这导致该解决方案的成本依然较高，有待进一步优化。2) 通过在相邻信道重新分配锁定资金的方式平衡信道，这一思路的典型方案有2017年提出的Revive[23]，其核心思想是组织支付信道网络中形成的环路，在环路上的信道之间实施重新分配锁定资金，该解决方案避免了链上事务，仅需环路节点参与，由选举产生的领导者主持平衡，整个过程可以无限次执行。但在闪电网络中存在大量不成环路的单支付信道节点，此类节点的再平衡问题在该解决方案里无法解决。针对此问题，近期上海交通大学的团队提出了Shaduf[24]，其核心思想是将相邻的支付信道以一条链上事务的代价链接，便可以在链接的支付信道间实现无限次再平衡操作。该解决方案有效解决了单支付信道节点的再平衡问题，但在设计方面依赖智能合约，因此目前只能应用于以太坊等图灵完备的虚拟货币，其通用性仍需进一步探索。3) 优化交易顺序的调度策略，避免不必要的单向拥塞。文献[25]提供了一种利用缓冲区为节点重新安排交易执行顺序的策略，有效减轻资金不平衡问题的发生概率。

3.4 节点实时在线假设

在目前的绝大多数支付信道网络协议中，通常假设支付信道里的节点均实时在线，在交易中双方都需要不断监控区块链，以确保对方没有发布过时的交易，而如果这一事件发生，诚实的一方需要迅速做出反应，并进行惩罚。然而节点实时在线假设在实际环境中是难以满足的，因此如果节点长时间掉线，例如停电或被恶意阻塞，则可能会被恶意节点利用，从而逃脱惩罚，损害诚实节点的利益。

为了避免这一情况发生，目前的解决思路有2种。1) 将退款和惩罚阶段所需的安全时间设定为一个较大的值。这种解决思路被绝大多数支付信道设计采用，当安全时间非常长时，诚实节点持续不在线的概率极低，敌手恶意阻塞成功的概率极小，因此避免了上述问题。但在该解决方案下，交易发生退款时解锁资金的等待时间较长，支付信道网络中大量资金处于被锁定的状态，这大大限制了信道网络的吞吐量。2) 文献[26]通过在闪电网络的基础上引入绝对时间T，确保用户只需在到期之前上线即可安全交易，并且给出了可直接应用于闪电网络的设计。但该方案仍然存在以下缺陷：引入绝对时间T使支付信道的生命周期出现了时间限制，一旦到期，即需要重新关闭和建立新的支付信道，从而带来额外的链上事务；同时，信道双方需要额外的抵押物，和闪电网络的原生架构相比，同样的交易需要锁定更多的资金。该解决方案虽然去除了节点实时在线假设，但也带来了新的挑战。

3.5 安全攻击

针对闪电网络的安全攻击主要包括虫洞攻击与悲伤攻击两类。

目前，解决虫洞攻击的主流思路是使路径中不同锁的释放互相独立，从而确保只有在前锁打开的情况下才能打开后锁，一旦跳过中间某一节点，其后续节点也无法开锁。文献[14]中给出了针对这一攻击的解决方案，其核心思想是：发送方通过匿名通信信道向交易路径上的每个节点发送随机化的信息，用于每个锁的生成和打开。在解开对应锁时将会泄露用于打开下一个锁的信息。由于各节点无法得知匿名通信信道中发送的信息，从而无法提前传递该信息以跳过中间节点。但该解决方案也存在新的攻击漏洞，即如果发送者与交易路径上的节点合谋，即可泄露信息并跳过某些诚实节点。

文献[27]本质上是探索支付信道网络设计签名方案的通用性，提出了基于BLS签名方案的支付信道网络方案，但也为上述问题提供了新的解决思

路，即发送方作为聚合签名中的一方参与到锁定资金过程中，既保障了资金锁定的独立性，又使发送者和路径上其他恶意节点无法共谋。但该解决方案需要额外的链上事务以保证安全，可能为区块链带来负担。文献[28]针对支付信道集线器的可扩展性进行研究，但该工作提出的基于同态加密的可随机化困难问题或能在上述问题中取得较好效果，期待看到更多该研究方向的工作。

另一方面，目前针对悲伤攻击的解决思路主要由工程方面的改善和改善协议设计两部分组成。1) 工程方面的改善思路包括缩短最长路由长度、对新节点降低最大并发HTLC合约数、避免路由环路等。2) 协议设计方面的改善包括设计快速响应和撤回的HTLC合约、缩短路径上资金锁定时间、避免路径上依次锁定资金等方向。文献[29]提出了用于原子多通道更新和减少锁定资金的协议，其在多通道应用环境下消除了悲伤攻击的放大因子，一定程度上可对抗悲伤攻击，对恒定锁定资金的支付信道网络设计有所启发。文献[30]提出了不需要依次锁定资金的一阶段提交的快速多跳支付协议Blitz，通过协议设计保证了恒定的锁定资金和更小的合同规模，虽然在退款时需要额外的链上事务，但也为协议设计方面提供了新的思路。

4　结束语

支付信道网络相关研究近年来逐步发展。本文对闪电网络的结构、安全性和隐私性进行研究，基于闪电网络存在的关键问题，总结梳理了近期支付信道网络的研究成果。对于每个研究方向，本文回顾和调研了最新的解决方案，并进行了详细的分析。基于观察和学习，本文讨论了当前基于区块链的支付信道网络设计中的发展和挑战，希望为后续相关研究工作提供灵感和支持。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.

[2] GERVAIS A, KARAME G O, WÜST K, et al. On the security and performance of proof of work blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 3-16.

[3] BELCHIOR R, VASCONCELOS A, GUERREIRO S, et al. A survey on blockchain interoperability: past, present, and future trends[J]. ACM Computing Surveys, 2022, 54(8): 1-41.

[4] WANG G. SoK: exploring blockchains interoperability[J]. IACR Cryptol EPrint Arch, 2021, 2021: 537.

[5] ZAMYATIN A, AL-BASSAM M, ZINDROS D, et al. Sok: communication across distributed ledgers[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2021: 3-36.

[6] GUDGEON L, MORENO-SANCHEZ P, ROOS S, et al. Sok: layer-two blockchain protocols[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2020: 201-226.

[7] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[EB/OL]. (2016-01-14) [2024-10-08].

[8] BONNEAU J, MILLER A, CLARK J, et al. SoK: research perspectives and challenges for Bitcoin and cryptocurrencies[C]//Proceedings of the 2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2015: 104-121.

[9] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: a scalable blockchain protocol[C]//Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2016: 45-59.

[10] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151(2014): 1-32.

[11] TAI S, EBERHARDT J, KLEMS M. Not acid, not base, but salt: a transaction processing perspective on blockchains[C]//Proceedings of the 7th International Conference on Cloud Computing and Services Science. Piscataway: IEEE Press, 2017: 755-764.

[12] TIKHOMIROV S, MORENO-SANCHEZ P, MAFFEI M. A quantitative analysis of security, anonymity and scalability for the lightning network[C]//Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Piscataway: IEEE Press, 2020: 387-396.

[13] KIAYIAS A, LITOS O S T. A composable security treatment of the lightning network[C]//Proceedings of the 2020 IEEE 33rd Computer Security Foundations Symposium (CSF). Piscataway: IEEE Press, 2020: 334-349.

[14] MALAVOLTA G, MORENO-SANCHEZ P, SCHNEIDEWIND C, et al. Anonymous multi-hop locks for blockchain scalability and interoperability[C]//Proceedings of 2019 Network and Distributed System Security Symposium. Reston, VA: Internet Society, 2019: 1-30.

[15] MIZRAHI A, ZOHAR A. Congestion attacks in payment channel networks[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2021: 170-188.

[16] KAPPOS G, YOUSAF H, PIOTROWSKA A, et al. An empirical analysis of privacy in the lightning network[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2021: 167-186.

[17] MANEVICH Y, AKAVIA A. Cross chain atomic swaps in the absence of time *via* attribute verifiable timed commitments[C]//Proceedings of the 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2022: 606-625.

[18] SUI Z M, LIU J K, YU J S, et al. Au_xChannel: enabling efficient bidirectional channel for scriptless blockchains[C]//Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security. New York: ACM Press, 2022: 138-152.

[19] SUI Z M, LIU J K, YU J S, et al. MoNet: a fast payment channel net-

work for scriptless cryptocurrency monero[C]//Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2022: 280-290.

[20] AUMAYR L, MAFFEI M, ERSOY O, et al. Bitcoin-compatible virtual channels[C]//Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2021: 901-918.

[21] ZHANG Y Q, VENKATAKRISHNAN S B. Rethinking incentive in payment channel networks[C]//Proceedings of the 2023 IEEE 43rd International Conference on Distributed Computing Systems Workshops (ICDCSW). Piscataway: IEEE Press, 2023: 61-66.

[22] SHARMA N, KAPOOR K, ANIRUDH V. Design and evaluation of Swift routing for payment channel network[J]. Blockchain: Research and Applications, 2024, 5(2): 100179.

[23] KHALIL R, GERVAIS A. Revive: rebalancing off-blockchain payment networks[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 439-453.

[24] GE Z H, WANG C K, LONG Y, et al. Shaduf: non-cycle and privacy-preserving payment channel rebalancing[J]. IEEE Transactions on Dependable and Secure Computing, 2024, PP(99): 1-18.

[25] PAPADIS N, TASSIULAS L. Payment channel networks: single-hop scheduling for throughput maximization[C]//Proceedings of the IEEE INFOCOM 2022 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2022: 900-909.

[26] AUMAYR L, THYAGARAJAN S A K, MALAVOLTA G, et al. Sleepy channels: Bitcoin-compatible bi-directional payment channels without watchtowers[J]. IACR Cryptol EPrint Arch, 2021, 2021: 1445.

[27] KRISHNAN T S A, MALAVOLTA G. Lockable signatures for blockchains: scriptless scripts for all signatures[C]//Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2021: 937-954.

[28] TAIRI E, MORENO-SANCHEZ P, MAFFEI M. A2L: anonymous atomic locks for scalability in payment channel hubs[C]//Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2021: 1834-1851.

[29] EGGER C, MORENO-SANCHEZ P, MAFFEI M. Atomic multi-channel updates with constant collateral in Bitcoin-compatible payment-channel networks[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 801-815.

[30] AUMAYR L, MORENO-SANCHEZ P, KATE A, et al. Blitz: secure multi-hop payments without two-phase commits[C]//30th USENIX Security Symposium (USENIX Security 21). Berkeley: USENIX Association, 2021: 4043-4060.

[作者简介]

徐秀（1992– ），女，山东临沂人，博士，中国信息通信研究院高级工程师，主要研究方向为密码应用、区块链、隐私计算、数据安全等。

田安琪（2000– ），女，陕西榆林人，中国科学院软件研究所博士生，主要研究方向为区块链技术。

何瑞雯（2004– ），女，北京人，中国科学院软件研究所硕士生，主要研究方向为密码学与安全协议。