支付通道网络的并发性和隐私性

孙徐炼3170102103

摘要：

像比特币这样的无需允许的区块链协议被固有的限制在事务吞吐量和延迟中。当前解决这个问题的手段集中在可以结合在支付通道网络（PCN）中的非连锁支付渠道，以使无需访问区块链就可以支持无限次数的支付而不是注册每个频道的初始和最终容量成为可能。当这种途径为低延误率和高的交易吞吐量铺路时，这种部署在实践中引起了一些对隐私问题的忧虑和与固定的交易中的自然并发性有关的技术挑战，而这个方面是人们没有深入研究过的。

在这个工作中，我们在支付通道网络中为隐私和并发性打好基础，为通用的组合性框架和可行受保护的安全问题解决提供了一个官方的定义。特别是，我们代表了Fulgor和Rayo。Fulgor是支付网络通道的第一个提供得证的隐私保证的支付协议，并且和比特币脚本系统完全兼容。然而，Fulgor是一个阻塞协议，所以容易在现场的支付通道网络的并发交易中出现死锁。与此相反的是，Rayo是支付通道网络第一个强迫无阻塞进程的协议（即至少有一个并行付款终止）。我们通过一种新的不可能的结果说明非阻塞进程必然以较弱的隐私为代价。Fulgor和Rayo的核心是多节点HTLC，一种新的智能比照，并且和提供有条件的交易的同时遵守就近原则减轻运行时间和沟通比特币脚本系统兼容。我们对Fulgor和Rayo的运行评估表明，一项经过10位中间用户的交易需要花费5秒，从而证明了在实践中部署的可能性。

CCS概念：

**安全和隐私-**对安全的要求；被破坏的系统安全；隐私保护

关键词：

支付通道网络；比特币；可扩展性；隐私；并行

**1 说明**

比特币是一种完全分散的数码加密货币网络，并且在当今世界已经被广泛应用为可选择的监察支付系统。这个系统的运作并非传统的在当地人们普遍信任的财务机构点清账目，而是在比特币区块链这个在相异的用户之间基于工作证明的全球共识算法相互复制的数据库上登录。虽然如此，这种共识算法的许可性质限制了交易率在每秒10次内，而诸如Visa这样的交易网络在最高时支持每秒47000次的交易量。

在最初对于比特币用户的增量和比较重要的交易的想法中，可扩展性被认为是当今比特币社区中主要关心的内容。多项调查和工业努力被暗示着克服这个主要障碍。

在比特币支付通道的使用意识到链下支付已经以受承诺的克服比特币可扩展性问题的方式繁荣起来。简而言之，双方用户通过向用比特币智能合同锁着比特币的区块链添加单个交易打开一个支付通道，然后多个链下交易就可以通过本地同意新的存款余额的分配来展开。最后，分享支付通道的用户施行另一个比特币交易来补充区块链中的最后的结余并快速关闭支付通道。

在这项任务中，区块链被要求开启和关闭一个支付通道，但这并不是在每项交易中的用户，从而减少了区块链的负担并增进了交易的输出。然而，这个简单的途径被限制在分享同一个开放通道的双方用户的直接支付上。引人关注的是，在原则上可能出现利用一个开放的支付渠道，从发送者到接收者有足够的能力来解决他们的付款的情况，事实上构建了一个支付通道网络。

还有很多困难需要被克服从而这样的支付通道网络能够适合逐渐扩大的用户和支付体系下大范围的调度的需要。特别的，我们从相似的支付系统如信用网络中知道，一个完备的支付通道网络必须提供很多问题的解决方法，这些问题包括：流动资金，网络结构，线路可扩展性，并行性和隐私等等。

比特币社区已经开始指出这些挑战，而现在的支付通道网络仍然不成熟，因为这些挑战需要深入的研究。在这项工作中，我们显示了这两个方面是互相联系并存在着一个固有的折中。

**隐私问题。**看起来支付通道必要地改进了比特币社区的隐私问题，因为它们不再是在区块链上登录的。然而，这样普及的想法开始被社区质疑，此时，支付通道网络能否提供高效的隐私保护也不甚明朗。最近的研究提出支付中心网络的隐私保护协议，在这里，每一位用户通过一个独一无二的中介来完成每一次链下支付。但不幸的是，人们不清楚怎样把这些解决方案推广到多节点支付通道网络中。

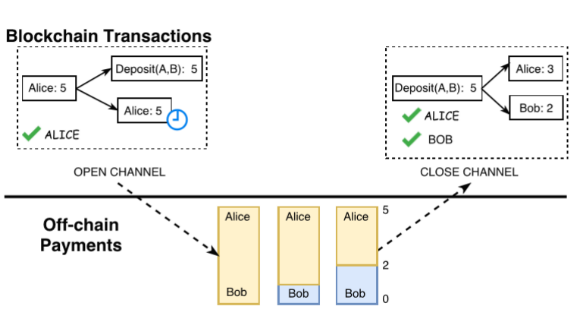
近几年有一些对于构建完备的支付通道网络做出的努力，在这些项目中，闪电网络已经成为比特币社区中的最佳支付通道网络。然而，它当前的操作并不能提供所有的支付通道网络中利益的隐私保护。比如，计算通过支付路径路由的最大可能值要求中间用户向发送者展示当前的支付通道容量，从而透露一些敏感的信息。另外，闪电网络中所用的比特币的智能合同强迫支付渠道中的原子为支付通道而更新，因而还要求揭露每个能被中间用户用来派生出谁向谁付钱的支付渠道中的用户的一般哈希价值。

事实上，在过多的学术论文已经研究了当今比特币区块链上比特币支付系统的隐私保护时，现在并没有支付通道网络提供或者符合其思想的严格的对于隐私保护的分析。对于他们自己的协议的严格定义的缺乏让这个模型和私人概念受到威胁，阻碍了官方对于正在进行的尝试的安全和隐私分析，更不用说得证的安全和隐私保护方案的发展了。

**并行问题。**一致的算法，如比特币中的工作量证明缓解了线上付款并行性问题中的序列化。在给定时间能够接近所有并行支付的挖矿机能够在数据被添加到区块链之前，在遵从一系列预先确定的规则下轻松序列化。然而，这早已不是仅仅在支付通道网络中出现的情况了：大多数链下支付都没有被添加到区块链中，因而不能在共识中序列化。此外，个人用户不能容易地解决并行性问题或者当这项交易可能涉及除了交易双方外的其他多个用户时。

在目前的支付通道网络，如闪电网络中，一旦路径中的一个交易通道容量不够大，这项交易就会瘫痪（可能被分派到其他正在并列运行的交易中）。而这就引起了死锁（和饥荒）的情况，并且，这个时候没有一个运行中的交易会结束。总之，尽管并行的交易可能在现行的支付通道网络按比例扩大到大量的用户和链下支付时发生，非继承的并行问题目前还没有被彻底地调查。

**我们的贡献。**这项工作达成了以下贡献：

1. 我们把支付通道网络中的安全和利益的私人概念官方化，命名为安全平衡，隐私价值和发送者/接收者匿名，这顺从了UC框架。
2. 我们第一次研究了支付通道网络中的并行性问题并展示了在Fulgor和Rayo两个系统用不同的策略解决问题。Fulgor是一个具备关于并行性问题解决方案的建议协调的区块协议，这些建议关于一些相似的支付网络比如会引起没有并行交易通过的死锁的信用网络。解决了这个困难，Rayo是第一个向支付通道网络承诺没有区块的进程的协议，通过这种方式，Rayo保证了并行交易中至少一个可以停止。
3. 我们描绘了一个饱受争议的惊人的支付通道网络中隐私和并行问题的权衡。特别的，我们阐述了任何实施非区块项目的支付通道网络必然在交易双方的匿名设置方面减少了，因此，隐私保障减弱了。
4. 我们官方地概括了多节点HTLC，这是一个建立在Fulgor和Rayo的核心上的智能合同，相比于闪电网络，保证了交易通道中从支付方到接收方的隐私，即使是对于其他用户。我们正式定义了多节点HTLC合同并提供了一个高效的最近被建议的零基础证明系统ZK-Boo实例化，这在之前“把要求的650MB的数据减少到17MB，把证明消耗的时间从600ms减少到309ms”的建议上有了改进。此外，多节点HTLC不要求比特币脚本系统的改变，就顺畅地在当前的支付通道网络中配置出来。这样，就有了独立的利益。
5. 我们已经在Python实施了Fulgor和Rayo的原型，我们还评估了实施交易所需要花费的执行时间和交流消耗。结果显示，有着是个中介用户的通道中的隐私保护交易可以在少至5秒是时间，在交流中引发17MB的间接费用。这表明，我们对于支付通道网络的协议和其他隐私保护交易系统相协调了。另外，我们的评估说明Fulgor和Rayo能够通过衡量来用合理的间接费用投合增长的用户的需求，这个间接费用之后还能通过优化实现减少。

**本文构成。**第二部分概述了所要求的背景；第三部分定义了我们处理这些工作和概述Fulgor和Rayo的过程中的问题，和我们为支付通道网络设计的隐私保护办法；第四部分详细地描述了Fulgor协议；第五部分概括了我们对支付通道网络的并行性问题和Rayo协议中细节的研究；第六部分概括了我们的运行和评估结果；第七部分讨论了相关的一些工作；第八部分则得出了此篇论文的结论。

图1：支付通道解说样例。白色实心方块代表比特币地址和当前的平衡，虚线方块代表比特币交易，时钟代表了一个定时合同，钩和旁边的用户名代表用户的交易验证签字，还有带颜色的方块代表支付通道的所处阶段，虚线箭头代表暂时的序列。那么这张图表示，爱丽丝首先拿出5比特币打开一个向鲍勃的支付通道，然后用这个通道向鲍勃链下支付。最后，支付通道以最近的结算关闭。

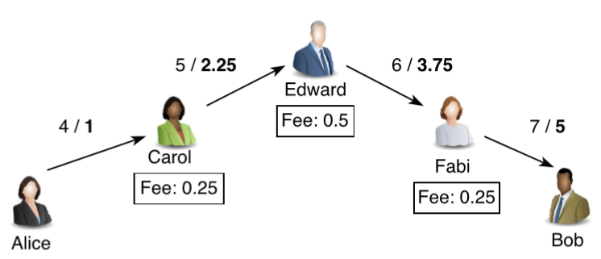


图2：支付通道交易的说明实例。不加黑（加黑）的数字代表了爱丽丝和鲍勃之间的交易发生之前（后）通道的容量。爱丽丝欲通过卡罗尔、爱德华、法比三人支付2单位比特币给鲍勃。因此，她用3单位比特币激活交易（即交易量加上运行费用）。

**2 背景**

在这个部分中，我们首先概括支付通道的概念，然后概括支付通道网络。

**2.1 支付通道**

一个支付通道在没有交付区块链中每一笔交易的情况下激活了两个用户之间的多个比特币交易，交易通道的基石是把比特币分配到多签名地址，这个地址同时被几个用户控制，这也保证了所有比特币在通道填满的情况下，在用户双方都同意的时间归还。接下来，我们概括了支付通道的基础，更详细的介绍，读者可以看[32，50，60]。

在图1的事例中，爱丽丝激活了通向鲍勃的一个最初为5比特币容量的支付通道，这个激活交易保证了爱丽丝在支付通道没有被使用的情况下能把钱拿回来。现在，爱丽丝可以通过按鲍勃的意愿调整订金结算后链下支付给鲍勃。每一项链下交易增大了鲍勃的结算而降低了爱丽丝的结算，当最后没有剩余的链下支付需求时（或者支付通道容量枯竭时），支付通道和区块链以一项关闭事务而关闭。这项事务以最近的支付通道中的结算为依据向每一个用户传送预订时所用的比特币。

图1中所展示的支付通道是单向通道的一个例子：这只在爱丽丝和鲍勃两人之间适用。双向通道则被定义为能够克服这个限制，因为链下交易对于两个方向来说都是可能的。双向支付通道在运行是实质上就像单向的一样运行，而这之中主要的技术难题在于改变通道的方向。在运行实例中，假设现行支付通道结算bal是{爱丽丝：4；鲍勃：1}，然后进一步假设鲍勃在链下向爱丽丝支付一单位比特币那么新的支付通道结算bal就是{爱丽丝：5；鲍勃：0}。在这一点上，爱丽丝从bal的结算中获得了利益，而鲍勃从bal中获取利益。这个矛盾的解决办法在于鲍勃和爱丽丝都确认任何先前的结算都在赞同最终结算的情况下失效。不同的“失效”技术已经在计划中，更详细的介绍，读者可以看[32，60，65]。

比特币协议已经更新以充分支持支付通道。特别的，交易可塑性和其他一系列引人关注的新特点都已经被加到了比特币协议中，同时也加入了隔离见证的应用。这个事件为不久后主要的比特币区块链上的实行和支付通道网络的试验做了铺垫。

**2.2 一个支付通道网络（PCN）**

一个支付通道网络可以用一个直接的图像G=（V,E）来指代，这里V即至高点（vertices），代表比特币数量；E即边缘加权（weighted edges），代表支付通道。每一个顶点u ∈ V和一个代表将会产生的费用的非负数相联系。直接的边缘加权(u1,u2)∈E代表了保留着的用户1支付给用户2的比特币。为了解释的方便，在接下来的论文中我们展示了一个用户1和用户2之间的双向通道，这里有两个边缘，每个方向都有一个边缘。这样的网络能够使用，然后在链下的双方用户的交易中运行，这时，他们之间没有开放的通道，但是通过开放的支付通道的路线联系起来。

两个用户之间交易的成功取决于连接两个用户的通道的可用容量和在这样的通道中所需要的费用。假设s想要向r支付α单位比特币，因而他们通过一个“s→u1→…→un→r”的路线联系起来。为了交易成功进行，每一个链接都有γi≥α′容量，其中α′i=α−Pi−1j=1 fee(uj)（即最初的支付价值减去通道上的中间用户索要的费用）。在一个成功的交易的最后，每一个从s到r的边缘都被α′i削减。为保证r得到精确的α单位的比特币，s必须以α∗=α+Pnj=1fee(uj)的价值开始本次交易。

在上述图2展示的交易说明实例中，假设爱丽丝想要向鲍勃支付2单位比特币，为此她需要用3单位比特币的价值来激活通道（2单位比特币加上路上用户索取的1单位比特币的费用）。这样，交易就这样进行了：链接爱丽丝→卡罗尔中的容量被减少了3，另外，卡罗尔以减少了2.75而不是3单位比特币的卡罗尔→爱德华链接中的容量索要了0.25单位比特币的费用。同样的，链接爱德华→法比被设置为3.75单位比特币的容量，链接法比→鲍勃被设置为5单位比特币的容量。

**2.3 最先进的支付通道网络（PCN）**

交易通道和支付通道网络的概念已经吸引了研究团队的注意，在运行中，比特币中存在多个正在进行的支付通道网络中介，这之中，闪电网络已经以比特币社区中最突出的例子启动了并且开始的中介已经在最近被发布了。支付通道网络的想法已经被提议来改进扩展性问题，不只是在比特币中，也在其他以区块链为基础的交易系统比如以太网中应用。

2.3.1 支付通道网络的途径。支付通道网络中一项重要的任务是在发送者和接收者之间找到一条容量足够的道路。在我们的设置中，每一个用户都了解网络中的拓扑学。这是每一个支付通道的打开都在公开的可用的区块链中登录的情况下的事件。另外，两个用户之间的悄悄话协议可以被执行以广播任何一个支付通道的存在。而且，每一个用户索要的费用也能以类似的方式公开。在这种情况下，发送者可以在本地计算发送者和接收者之间的路程。在接下来的论文中，我们假设发送者以她自己的标准选择路径。不过，我们把路径选择看成一个引人关注却正交的问题。

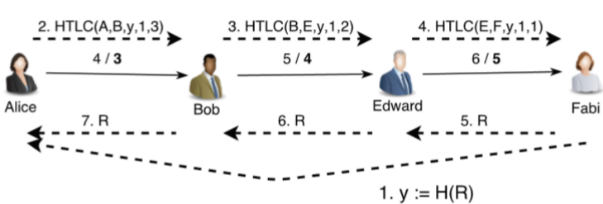
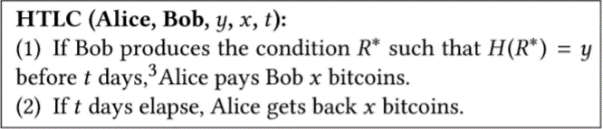


图3：1价值的HTLC合同下的从爱丽丝到法比的交易的说明实例。第一，这个状况从爱丽丝被传送到法比，然后在用户之间前进，在每个支付通道中拿1单位比特币.最后，接收者出示R，释放所有刚才在支付通道中拿的比特币。简单起见，在这个例子中，我们假设了没有交易费用的消耗。

2.3.2 支付通道网络中的交易。沿支付通道开展的交易通过依据交易量和相关费用更新每一个通道的容量而被执行（见2.2）。这样的操作引起了一个重要的原子数的挑战：要么路径上所有通道的容量被更新，要么没有一个通道被改变。只允许路径中的一些通道改变会导致用户的比特币损失（即一个用户会支付一定数量的比特币给下一个用户但从未收到前面相邻用户的比特币相应的比特币）。

当前闪电网络的提议由一个叫做哈希时间锁合同（HTLC）的智能合同组成。这个合同会锁住x单位的比特币，而只要合同是满足的，这x单位比特币就能被释放出来。这个合同以哈希价值的形式y:=H(R)被定义，R是被一致地随意选择的，x的值和时间t，像这样：



一个HTLC的使用说明实例在图3中进行了描绘。为简单起见，我们假设没有交易费用的消耗。第一，交易额度（即1单位比特币）在发送者到接收者的设置中给定的，之后又从接收者释放到发送者。更具体点，也就是说，接收者（法比）向发送者（爱丽丝）发送了条件，爱丽丝和她相邻的用户设置了HTLC，高效地控制了交易价值（即1比特币）。这样的HTLC之后在每一个通向接收者的路径中被设置了。在这点上，接收者知道交易价值在每一个支付通道中都被控制，所以她揭示了R价值，这让她能够满足合同以解决路径上每一个支付通道的新增容量。

需要重点指出的是，通道中每个用户都在流出支付通道中设置了HTLC，这项进程用了一个比进入支付通道小的时限。在这项活动中，用户需确定她能够在自己的比特币转移到后一用户后把比特币从前一用户转移过来。链下的用户可以外包和与她的支付通道相关联的HTLC合同相一致的监督的实行。

尽管HTLC与比特币完全兼容，它的使用施行导致了一个重要的隐私问题顶峰：看到每个用户参与具体的交易时的哈希H(R)价值都能被辨认。第一，路径上两个相连的用户能够直接推导他们参与了这项交易这一事实的产生，且这之中可以被利用的是重新架构发送者和接收者的身份。第二，如果HTLC的陈述上传到了区块链（即由于交易通道上是非协作的中间用户），即使她不是交易中的参与者，观察员可以轻易地跟踪整个用于交易路线设定的路径。我们提出了一个异常的多节点HTLC智能合同在没有中介用户损失比特币的情况下避免隐私问题的产生。

而当今支付通道网络的研究中重点涉及的一个问题是并行交易的运行，这些并行交易要求在路径上共享交易通道，现今的提议是在支付路径上的共享通道的结算不足时简单地中止交易，然而，就像我们在3.3中所展示的，这个方法会导致死锁，在这个死锁中，没有一个同时进行的交易终止。我们提出一个保证没有区块的协议，那就是多个并行交易至少有一个终止。另外，我们展示了一个并行和隐私之间与生俱来的平衡，这个平衡适于任何完全分配的交易网络。

**3 问题解说**

在这部分中，我们首先把支付通道网络和潜在的操作形式化，然后讨论攻击模型和我们的安全、隐私目标。接着，我们会概括一个理想的提议下的功能世界，并展示一个系统的概括。在整个接下来的描述中，我们不妨假设每一个计算都是区块链的输入，且是向所有用户公开的。

定义3.1（支付通道网络（PCN））。支付通道网络被定义为图像G:=(V,E)，其中V是比特币账户的设置，E是最近开启交易通道的设置。支付通道网络相对于区块链B来定义，且被配置了三项操作（开放通道，关闭通道，支付），一下是概要：

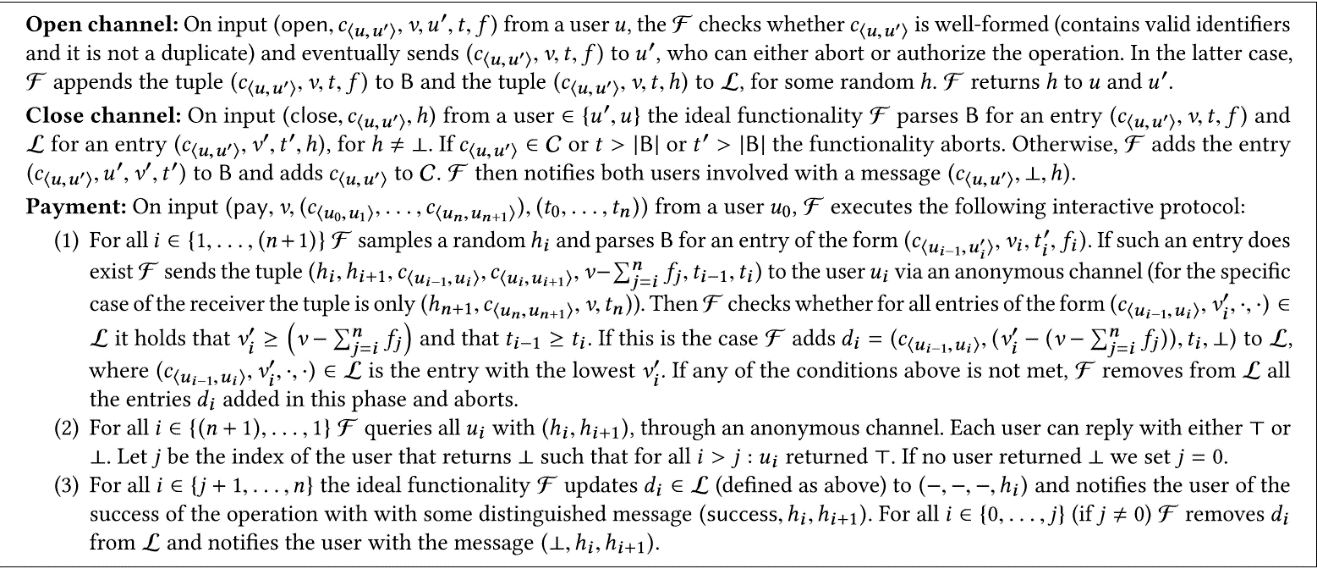
* 开放通道(u1,u2,β,t,f)→{1,0}。在输入时两个比特币定位了u1,u2∈V，一个最初的通道容量β，一个时间余量t，和一个消耗价值f，如果操作被u1授予，那么u1就用于至少β单位比特币，发放通道创造了一种新的支付通道(c⟨u1,u2⟩,β,f,t)∈E，这之中c⟨u1,u2⟩是一个新的通道标识符，然后这个标识符上传到B，再回到1。否则，它回到0。
* 关闭通道(c⟨u1,u2⟩,v) →{1,0}。在输入一个通道标识c⟨u1,u2⟩和一个结算v（即通道中被锁住的比特币在u1和u2之间的分配）时，如果操作同时被u1和u2所授权，关闭通道会从G转移一致的通道，包括B中的结算v和返回1.否则，它回到0。
* 支付((c⟨s,u1⟩,...,c⟨un,r⟩),v) →{1,0}。在输入时，那一连串的通道识别器(c⟨s,u1⟩,…,c⟨un,r⟩)和一个交易价值v，如果交易通道组成了从发送者（s）到接收者（r）的一条路径，并且路径上每一条通道c⟨ui,ui+1⟩都已经至少有一个当时的结算γi≥v′i，此时v′i=v−Pi−1j=1fee(uj)，而v′i支付操作降低了当时每个支付通道c⟨ui,ui+1⟩的结算并回到1。否则，交易通道中没有一个结算可以被更改，然后交易操作就回到了0。
  1. **攻击者模型和安全、隐私目标**

我们考虑一个计算上有效的攻击者，这个攻击通过大量生产用户和腐化任意应用的潮流影响她的网络的形成。一旦一个用户被毁坏，它的内部阶段就会被传递到攻击者，然后这个用户所有的接下来的信息都被传递到攻击者手中。另一方面，我们假设两个不妥协用户之间分享交易通道的交流是机密的（即通过TLS）。最后，攻击者可以代表被毁坏的用户发送随意的信息。

为了对抗以上敌手，我们明确了接下来的这个利益下的安全和隐私概念：

* **结算安全。**直观的，结算安全保证了任何参与了交易过程的诚实的中介用户（就像定义3.1中具体描述的）即使是在所有支付操作中其他用户都被毁坏的情况下都不会损失钱币。
* **可串行性。**我们要求支付通道网络的执行都是可串行的，即对于支付操作的每一个并发的执行都有等价的相继的执行。
* **（链下）隐私价值。**直观的，隐私价值保证了某项支付操作只涉及诚信用户，排除在交易路径外的被毁坏的用户则无从知晓和交易价值有关的任何信息。
* **（链上）关联匿名[24，59]。**关联匿名要求给出两个同时发生的(payi((c⟨si,u1⟩,…,c⟨un,ri⟩),v))i∈[0,1]组成下的成功交易事件，且其中至少有一个诚信用户uj∈[1,n]，被毁坏的中介用户不能为给定的可能性大于1/2的交易payi决定组成(si,ri)。
  1. **理想世界功能**

**我们的模型。**网络的用户被看成交互式的模型，一个受信任的功能F和图灵机通过安全和已认证的公道来交流，然后我们把模型中的攻击者A看成一个概率多项式时间机，且这个A被给出了额外的向系统增加用户同时毁掉这些用户的交流功能。A可以适应性的在任何时间对此交流表示怀疑，在毁坏一个用户u的时候，攻击者可以得到u的内部情形的信息，这样，接下来将要执行的用户u交流都完全是通过A来实现的。

**假设。**我们按理想功能Fanon（在[26]中有所介绍）构造网络中任意两个用户之间的匿名交流模型。进而，我们假设区块链B的存在，这是一个受信任的加属性公告板（例如[72]），一致的理想功能FB留在B并根据用户之间的交易而更新。在执行过程中的任何时候，支付通道网络中的任何用户都可以向FB发送一个可辨认的消息，而FB把整个交易从B发送给u。我们定义了B的所有条目的数据量是|B|，在我们的模型中，时间和区块链B的条目数据量一致，即时间t是任何|B|=t时的时间。我们理想化的过程F把Fanon和FB当成潜在路线，即我们的协议具体为(Fanon,FB)的混合模型。这里指出我们的区块链模型是一个现实的粗糙的纹路抽象图，所以更多的精确的组成可见于文学，见[44]。为容易阐述，我们就定位于这个最简单的视角，但是人们通常容易把我们的模型扩大到合并复杂的抽象概念。

**注释。**区块链B中的交易通道都符合(c⟨u,u′⟩ ,v,t,f)的组成，其中c⟨u,u′⟩是一个独特的通道标识符，v是通道的容量，t是通道终结的时间，f则是相关费用。为注解的方便，我们假设用户(u,u′)的标识也被编码为c⟨u,u′⟩，我们要强调的是任何两个用户中都有可能会有多个通道同时开启。这个功能在另外两个列表C和L中保留着。前者是用来跟踪关闭的通道的，而后者用来记录链下交易的。L的条目符合的是(c⟨u,u′⟩ ,v,t,h)，其中c⟨u,u′⟩是一致的通道，v是已用的信用数，t是交易终结所用的时间，而h是这个条目的标识符。

图4：支付通道网络的理想世界功能

**操作。**在图4中我们概括了F和支付通道网络的用户之间的相互作用。简单的说，我们建立了单向的通道模型，尽管我们的功能会被轻易扩大到支持双向通道。我们同时事件的执行者从F开始，并将本地的空白列表(L,C)初始化，支付通道网络的用户可以向F提出疑问来开启通道并在L的任何一个有效级关闭它们。在输入时，对于价值v和一系列从u0开始的支付通道(c⟨u0,u1⟩,. . .,c⟨un,un+1⟩)，F都会检验这个路径是否有足够的容量（步骤1），然后开启交易。每一个中介用户可以选择要么允许交易，要么否认它。而交易一抵达接收者，每一个用户都可以再次决定是否打断资金的流动（步骤2），即支付而不是发送者。最后，F通知涉入成功操作的交叉点（步骤3），为了达到一致，还要把更新的阶层添加到L。

**交流讨论。**在这里，我们展示出我们的理想功能为支付通道网络捕获利益下的安全和隐私性质。

* 结算安全。把ui看成交易的支付((c⟨s,u1⟩,. . .,c⟨un,r⟩),v)中的任何中介点，F把与即将到来和正在进行的ui一致的边缘在本地上传到L，这样，全部的ui结算都会因她在费用重点设置增加,除非用户的活动拒绝它（步骤2）.因为F是受信任的，所以结算安全遵循它。
* 可串行性。考虑到在此时只有单跳交易，我们很容易看到理想功能会串联执行，即任何两个并行交易只能在不同的链接上发生。因此我们可以普遍发现一个在一系列指令下重复相同操作的制表员（即在任何指令下）。通过结算安全，任何交易都可以被一系列微粒的单跳交易代替，因此可串行性可以承受。
* 评估隐私。在理想世界中，交易路径上不撒谎的用户都没有与F联系，因此他们不知道任何和交易有关的信息（对于链下交易）。
* 关联匿名。让ui成为交易中的一个中介交点，在交互作用中，ui只得到了每项交易中的一个独特标识符。特别的，这样的标识符是完全从同一个交易中的其他用户的标识符独立的。接下去就是，只要交易路径上有至少一个诚信用户ui撒谎了，任何两个相同路径上的有着相同价值v的同时的交易都对用户ui+1的不可分辨。这暗示了任何被毁坏的中介交点的适宜子集为任何两个成功的并行交易会跨越所有的被毁坏的节点，不能辨认在哪个命令下促进了交易的进行。因此，这样的一系列被毁坏的节点不能决定正确的发送者—接收者对可能比1/2好。

**UC-安全。**让EXECτ, A,E成为当对手A和执行协议τ的当事人环境E的输出的总效果（对于所有涉及到的机器的任意比特币）。

定义3.2（UC安全）。协议τ uc意识到一个理想的能力F如果对于任何对手A都有一个模拟器S那么对于任何的环境E，总效果EXECτ ,A,E和EXECF,S,E都是计算上不可分辨的。

**支付通道网络中和拜占庭式用户的较低联结。**我们观察到在支付通道网络中包含了两个用户都是拜占庭用户的通道(à la malicious)[46]，并行中存在着一个固定的费用。具体的，在这个支付通道网络中，如果我们提供了非区块的过程，即至少一个并行的交易会结束，这样在支付通道网络中提供串联就不可能了（比较附录D中图11）。这样，今后，此文中所有的结果和要求都假设了在任何支付通道网络的执行中都有一个用户双方都是拜占庭用户的通道。

引理3.3 如果一个交易通道中的双方用户都是拜占庭用户，那么对于提供非区块过程的支付通道网络问题没有串连协议。

* 1. **核心观点和系统概述**

接下去，我们对我们在支付通道网络中如何达到隐私和并行交易给出一个高层次的概述。

3.3.1交易隐私。支付操作必须保证支付通道网络中利益下的安全和隐私所有权也就是结算安全，隐私价值和关联匿名。一个达到结算安全的天真的途径可能是HTLC基础上的交易（见2.3.2）。这个解决办法是无论和匿名有怎么样固有的矛盾：都很容易看到，属于同一个交易的合同在每个人之间相联系，因为他们在相同的状况（h）下被编码来释放支付。我们的提议多节点HTLC的目标就是在和比特币网络保留完整的兼容性时除去这个节点间的关联。

这个建立在多节点HTLE之上的想法是这样的：在n节点交易最开始，发送者把n多个独立的线(x1,…,xn)作为样本，然后，对于所有的i∈1,…,n,她设置了（公式略），其中H是随意的哈希功能。也就是，每一个yi是在XOR组合器提供功能H给所有输入价值xj（j ≥I ）的结果。发送者接着向接收者提供了(yn,xn)和第i个节点和元组(yi+1,yi,xi)。为了保护匿名，发送者和通过匿名通道把价格传递给中介节点。从发送者开始，每一对相邻节点(ui+1,ui)都会在输入(ui,ui+1,yi,b,t)中定义HTLC标准，其中b和t分别是比特币数量和时间参量。这里指出合同的释放状况被一致地在功能H的范围中被划分，因此，单个交易的HTLC是彼此独立的。很清楚的是，这个原理很好地概述了上文的工作，只要发送者根据协议的说明书选择了每个价格yi。我们还可以通过非交互的零知识证明强制诚信行为[38]。

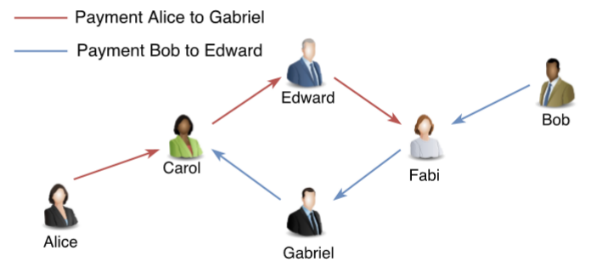


图5：两个区块的交易实例：爱丽丝到加比利埃尔（红色）和鲍勃到爱德华（蓝色）。简便起见，假设每个交易支付1比特币且每个交易通道有1单位比特币的容量。每个交易通道以先到达那一方的颜色着色。在这个死锁情形中，没有一个交易可以在路径上前进了，而且完全不能成功。

3.3.2 并行交易。在没有一个交易穿过的行为中，两个（或更多）同时的交易在交易路径上共享一个支付通道是可能发生的。在图5描述的例子中爱丽丝到加布里埃尔的交易不开展是因为从法比到加布里埃尔的支付通道的容量已经被鲍勃和爱德华的支付锁上了。另外，这个第二项交易在卡罗尔和爱德华之间的支付通道已经被锁住时亦不能开展。这个死锁状况是支付通道网络中一个常见的问题，此时，一旦路径上有一个支付通道没有足够的容量了，交易就会被中止。

**区块支付(Fulgor)**。尽最大努力能够给出的解决办法以防两项交易都失败而构成这个死锁。被中断的交易不影响相关用户的结算，因为接收者不会公开被锁交易通道的释放状况。因此，相关的交易通道只有在一致的时间过后和比特币被送回最初的拥有者之后才会被解锁。

所有被中止交易的发送者之后可以随意地选择一段时间等待后重新发行这项交易。尽管这个区块机制极像其它交易网络例如Ripple或SilentWhispers中用户的操作，这可能降低交易在完全分散的支付通道网络中的生产量。

**非区块支付（Rayo）。**一个可选择的解决办法由非区块解决办法构成，在这里，一系列并行交易中至少有一个完成交易。我们在通向达到这个目的的路径中假设有交易的整体序（即通过一个整体交易标识）。概括地说，用户们可以排队支付，排队时，比当时有较高的标识的交易进入通道进行交易，较低的则被中断。这保证了要么当前正在进行的最终 完成，要么排队的交易中的一个最终完成，因为它们的标识较高。

1. **FULGOR：我们的解释**

在这个部分中，我们介绍关于密码的建设区块，这在我们的解释（4.1）中有要求，我们概括了多节点HTLC合同的一些细节（4.2），还讲了支付通道网络操作的建构的细节（4.3），计算了安全性和隐私（4.4）并用一些记号来得出结论（4.5）。

**符号。**我们用λ表示我们的系统的安全系数，用标准定义表示一个几近可以忽略的功能，我们还用decision表示在一项交易的支付通道中可能发生的事件，这个decision是为与交易价格相一致而锁住交易通道的结算的正向信号。而decision放弃因交易失败被锁住的资金信号的释放一致地，decision接收接收者收到付款的确认信号。

为了解释的方便，我们假设用户的标识(ui,ui+1)可以从通道标识c⟨ui,ui+1⟩中提取出来。

**系统假设。**我们假设支付通道网络中的每一个用户都了解完整的网络拓扑学，也就是所有用户的设置和每一对用户之间存在的支付通道。我们进一步假设交易中的发送者根据她自己的判断来选择通向接收者的支付通道。当前每一个交易通道的价格没有公开，而是被共享通道的用户保留在本地，因为否则，隐私会被琐碎地破坏。接着，我们再假设每一个用户都知道支付通道网络中每一个用户都会索要交易费用。

这可以在练习后达成。两个用户之间的支付通道的开启要求添加一个区块链中的交易，并且这项交易需要含有此二人的标识。因此，支付通道网络中的拓扑学是有琐碎的漏洞的。此外，用于打开交易通道的交易可以包含用户定义的数据[5]，因此每个用户可以决定自己的交易费用。在这个行为中，每一个用户可以主动地收集更新的网络拓扑的信息和区块链本身的费用或者被潜在的协议散播[48,62]。

现在我们再假设一对分享交易通道的用户通过安全的已验证的通道（比如TLS）来传输信息，这样，给出每一个用户在公共锁下都有特殊标识很容易实现。我们也假设某项（可能是间接的）交易的发送者和接收者可以通过安全和直接的通道传输信息。最后，我们假设交易的发送者能够和每一个中介用户创造一个匿名的支付通道。可以用于到达每个用户的IP地址可以在创造交易通道中被编码，因此登录到了区块链中。我们指出我们的协议在路线方面是完全参数化的，因此任何洋葱路线一样的技术会在本文中运作起来。

我们考虑绑定的同时的传输设置[23]。在这样的传输模型中，时间被划分成了确定的传输循环，并且我们假设某个回合中所有某个用户发送的消息都是接收者不需绑定的执行中的数据步骤就可以得到的。因此，消息的缺失暗示了在循环中用户的传输的缺失。在练习中，这可以通过支付通道网络的用户之中宽松的同步时钟来达到。

最后，我们假设有一个用户中完整的命令（即被公开确认的键编了词典分类的）。

* 1. **建筑区块**

**非交互零知识。**令R:{0,1}∗×{0,1}∗ → {0,1}为NP联系，并令L为R的一套正面实例，即L={x|∃ws. t. R(x, w)=1}，一个R的非交互零知识证明由从证明P到校验者V的单个信息组成，证明者P想要计算一个证明π，这个π使校验者确信，某个特定的阶段x ∈L。我们允许证明者继续一个额外的输入w，这样，就满足R(x, w) = 1。校验者可以选择接受或拒绝，这取决于π。如果V总是接受陈述x ∈ L下的诚信计算得到的π一个NIZK是完全的，而如果除了可忽略的偶然性,V总是拒绝所有x < L下的任何π是可靠的。宽松的讲，如果在x ∈L的事实外，检验者没有从π得到任何信息的NIZK证明就是零知识。高效的NIZK协议被了解是在随意的预言模型中存在的[38]。

双方用户之间的协议。用户ui和uj共享了一个交易通道，在本地保留被定义为信标器通道状态:= cap(c ⟨ui ,uj⟩)的交易通道状态，其中信标器通道状态表示了当前的支付通道容量。我们要求一个双方团体协议来保证两个用户同意了当前在每个点的及时价值cap(c ⟨ui ,uj⟩)。我们在附录B中概括了这种协议的细节。为了本文的可读性，接下来我们暗中假设共享一个交易通道的双方用户对当前状态是满足的。

* 1. **多节点HTLC**

我们考虑从发送者Sdr到接收者Rvr在某个价格v下通过用户(u1,...,un)的通道的非直接交易标准的设想其中un=Rvr。属于同一个网络的用户共享了哈希功能H:{0,1}∗ → {0,1}λ的概念，我们塑造为任意的预言。

令L为下面这种语言：L = {(H ,y′, y ,x) |∃(w) s.t.y′ = H(w)∧y = H(w ⊕x)}，其中w ⊕x代表两个比特串的按位XOR。在交易开始之前发送者Sdr在本地执行了图6中所展示的HTLC设置算法。

直观地看，发送者样本是n个随机的xi和（公式略）定义yi，这是所有xj（j ≥i）的XOR集合。接着，Sdr计算了π证明来保证在没有暴露所有xi的情况下每一个yi是符合语法的。接收者被提供了(xn,yn)，这样她只需简单的核实yn = H(xn)，Sdr接着通过一个直接的发送通道发送(xi ,yi ,πi)到每一个中介用户ui。每一个ui运行V((H,yi+1,yi,xi),πi)，并且，如果确认算法驳回了证明，就要中止这项交易。

从u0 = Sdr开始，每一对用户(ui,ui+1)核实是否双方用户都从(yi+1,v)接收到了相同的价格。这可以通过简单的交换和我比较两个价格来完成。如果是在这个案例中，他们建立2.3中那样的HTLC (ui, ui+1, yi+1, v, ti)，这之中，ti定义了一些时间间隔，这样，对于所有满足i ∈ [n] : ti−1 = ti + ∆的r，有若干正面价值∆。一旦(un−1,un)间的合同定下来，用户un（接收者）接下来就能通过释放xn来推动v单位比特币的前进，这在原则上能够满足约束H(xn) = yn。而一旦xn被公开，un−1也能通过简单的xn−1 ⊕xn输出为(un−2,un−1)之间的合同释放有效的条件。实际上，这个体制在每位交易路径上的中介用户间转播，直到Sdr：对于每一个节点ui，都有代表无论何时(ui,ui+1)之间的合同的条件被释放，即有人公开了串r，这样就有了H(r) = yi+1，接着ui立即了解了xi ⊕r，则H(xi ⊕r) = yi，这是一个(ui−1,ui)之间合同的有效条件。接下去要说的是中介用户，每个中介用户的向外的合同已经被推动了，他们能够为向内的合同释放有效的条件。

* 1. **解释细节**

接下来，我们概括构成Fulgor的三个操作（开放通道，关闭通道，支付）的细节。

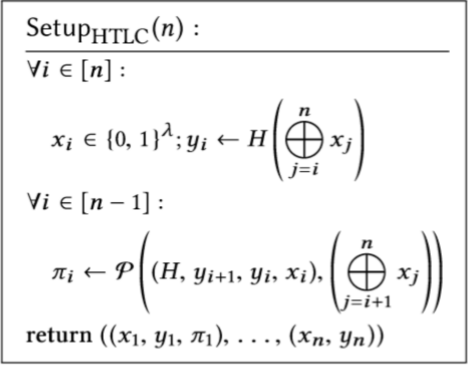


图6：为多节点HTLC合同建立一个操作。

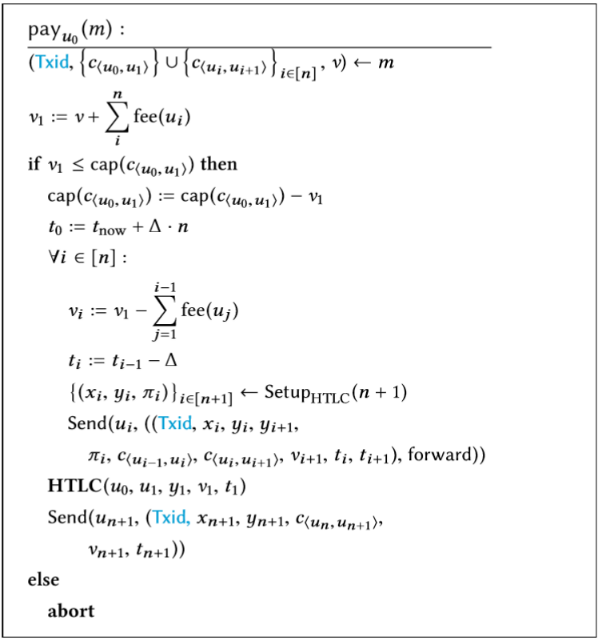


图7：Fulgor中发送者的支付路线，亮蓝色的伪代码展示了在Rayo中额外要求的步骤。

* 开放通道(u1,u2,β,t, f )：这个操作的目的是开启一个从u1到u2的通道，为此，他们创造了一个最初的比特币存款，其中包括以下信息：最初的通道容量（β）、通道的时间限制（t）、使用通道收取的费用（f）以及双方用户提前达成一致的通道标识符(c⟨u1,u2⟩)。在比特币存款以及被成功加入到区块链中后，操作就回到了1，如果任何一个先前的操作没有按规定执行，这个操作就回到0。
* 关闭通道(c⟨u1,u2⟩，v)：这个操作被共享一个开放的交易通道的双方用户(u1,u2)用来在到达由v规定的情况的时候关闭它，并有根据的更新比特币区块链中的比特币结算。这项操作在Fulgor中以在最初支付通道（见2.1）的提议中被规定的方式运行，另外，当且仅当一致的比特币加以被加到比特币区块链中时，操作回到1。
* 支付((c⟨u0,u1⟩,...,c⟨un,un+1⟩),v)：一个支付操作交易通过双方之间的一条开放交易通道(c⟨u0,u1⟩,...,c⟨un,un+1⟩)从发送者（u0）向接收者（un+1）传递了一个价格v，在这里，我们概括了支付操作的一个区块版本（见3.3）。我们讨论第五部分中支付操作的非区块版本。

像图7中（黑色伪代码）所展示的，发送者首先计算以v1：= v +∑ifee(ui)发送v单位比特币到Rvr所需的费用，然后是在交易路径上的与每一个中介节点一致的费用。如果发送者没有足够的比特币，她会中断交易。否则，发送者为每一个交易通道上的中介用户拟成一份合同，这遵从了4.2中概述的机制，并且向相应的用户发送了信息。

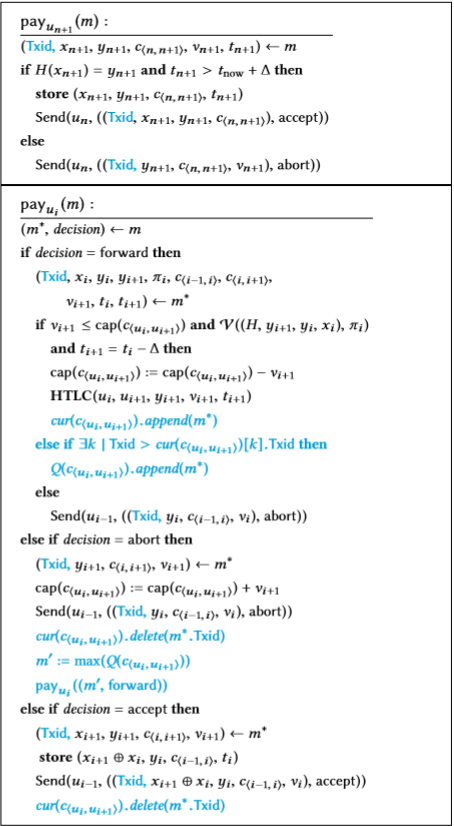


图8：Fulgor中对于接收者和所有中介用户的支付路线。亮蓝色伪代码表示Rayo中额外的步骤。Max（Q）以Q中最高的标识符送回交易中的信息。

每一个中介用户会核实即将发生的HTLC有一个比交易通道的容量少或者与其相等的和路径上的后续用户相关的价格。另外，每一个中介用户还核实与即将发生和正在发生的交易通道中的HTLC的零知识证明和即将发生的HTLC的时间限制以及和现行的HTLC的区别∆。如果这样，她就与路径上的后续用户为相同的相关价格生产了相应的HTLC（可能是减去费用的）；否则，她就会通过向路径上前一位用户引发中止事件的方式中断这项交易。这项操作已经在图8中得到了展示（黑色伪代码）。

如果路径上的每位用户都接受这项交易，这项交易就会最终到达接收者，接收者就转而释放所要求的信息来填补路径上的HTLC（见图8（黑色伪代码））。有趣的是，如果所有中介用户都中止这项交易，接收者就不会释放条件，因为她没有受到任何付款。此外，在路径中先前的节点已经被设置好的交易通道在HTLC对应的时间限制过后会变成空的。

* 1. **安全和隐私分析**

接下来，我们陈述了Fulgor中的安全和隐私结果。我们在(Fanon, FB)-hybrid模型中证明我们得到的结果。也就是说，定理4.1适用于任何Fanon和FB中UC-安全的实现。我们在附录A中展示定理 4.1的证明。

定理 4.1 （UC-安全）。令H：{0,1}∗ → {0,1}λ为被做成任意预言模型的哈希功能，并令（P,V）为一个零知识证明系统，然后Fulgor的UC了解了(Fanon, FB)-hybrid模型的图5中描述的理想功能F。

* 1. **系统探讨**

**与比特币的兼容性。**我们指出所有的无标准密码操作（比如NIZK证明）在链下发生，同时唯一被要求在区块链核查中执行的算法是可以和SHA-256实例化哈希功能H。因此我们的多节点HTLC体制和Fulgor整体上和当前的比特币脚本是完全兼容的。此外，就像2.1提到的，SegWit或比特币中可锻性问题的相似解法的加法在比特币系统中完全使支付通道成为了可能。

**概论。**Fulgor是一般的支付通道网络（不仅与比特币联结）。Fulgor要求：(i)开放通道允许植入顾客数据（即费用）；(ii)交易通道中有条件的结算更新。作为算法数据可以包含在加密货币交易[5]中，且在其他合同中，大多数支付通道网络支持HTLC合同，而Fulgor也可以在其他很多支付通道网络比如Raiden中使用，这是为Ethereum[13]设计的支付通道网络。

**双向通道支持。**Fulgor可以被轻易地扩大以支持双向交易通道和仅有的两个次要的改变。第一，交易信息必须包含，每一个交易通道所要求的方向。第二，通道c⟨uL,uR⟩的容量是价格(L,R,T)的元组，其中L表示当前的uL结算，R是当前的uR结算，而T是通道全部的容量。价格为v的从左到右的交易在L ≥ v且R + v ≤ T的情况下是可能的。在这种情况下，元组被更新至(L−v, R + v, T)，从左到右的交易就被相应地解决了。

1. **支付通道网络中的非区块交易**

在这部分中，我们讨论在非区块的行为中怎么解决并行交易的问题。也就是怎么保证一系列并行交易中至少一项交易完成。

接下来，我们从一个不可能的指导了Rayo的设计的结果出发，还有我们在非区块交易方面的协议。然后，我们概括了在理想世界中要求的改进功能和Fulgor来达到要求。最后，我们讨论这些改进的隐私属性的含蓄之意。

* 1. **并行 vs 隐私**

我们展示了达到非区块进程要求一个和每一项交易有关的全球的状况。具体的，我们展示了我们无法为支付通道网络提供不相交访问并行性和非区块过程。正式的来讲，如果对于任意两个交易通道ei，ej，channel-state (ei)∩channel-state(ej)=∅ ，那么支付通道网络执行就是不相交访问并行的。

引理5.1 在提供非区块过程的支付通道网络中，严格系列化的不相交访问并行执行不存在。

我们把证明草图延缓到附录D去看。我们已经因并行和隐私问题建立了这样一个固有的费用机制，我们又把全球状况模型化为和每一项交易有关的Txid领域。但我们要备注的是这个Txid允许敌手减少可能的交易中的发送者和接收者，因而必然降低了隐私的保证，就像我们在5.2中所讨论的。

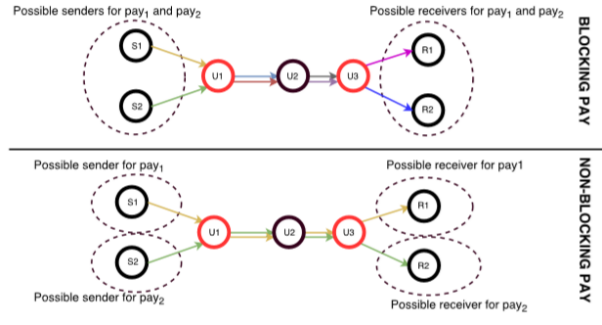


图9：这是一个并行和隐私间交易的实例。每一个节点代表一个用户：黑色吗的节点代表诚信用户，红色节点代表拜占庭用户。在这两种情况中，我们假设这两个并行的交易：S1支付给R1和S2支付给R2通过U1，U2，U3来实现。箭头的颜色表示支付标识，虚线椭圆代表每一个事件中的匿名集。

* 1. **理想世界功能**

在这里，我们展示怎样修改3.2中讲到的理想的功能F来说明达到任意支付通道网络中的非区块过程。第一，单个的标识Txid（而不是一个样本化的hi）被用于路径(c⟨u0,u1⟩,...,c⟨un,un+1⟩)上的所有支付通道。第二，F不再简单的在支付通道没有容量时中断交易，而是把交易排队，如果交易的Txid比当前的高就提上去，比当前的低就中止。我们在附录C中详细介绍了改性的理想功能。

**讨论。**在这里，我们讨论改性的理想世界功能怎样捕获利益下的安全和隐私概念，如3.1中所述。特别的，我们很容易看到结余安全和价值隐私被推动到同一个轨道上。然而，同一交易标识在交易路径上所有中介用户间的泄露把可能的发送者和接收者降低到实际的发送者和接收者，从而打破了相关匿名机制。因此，怎么解决并行交易（区块和非区块）和匿名保证间存在着固定的交易。

在图9中就展示了这个交易的实例。它说明了两个同时的交易pay1((c⟨S1,U1⟩,c⟨U1,U2⟩, c⟨U2,U3⟩,c⟨U3,R1⟩),v)和pay2((c⟨S2,U1⟩,c⟨U1,U2⟩,c⟨U2,U3⟩,c⟨U3,R2⟩)如何取决于在区块或非区块的状态下并行交易被解决。我们假设这两个交易能够在当前的支付通道网络中完成，且这两项交易传递了同一个交易数额v，否则，关联匿名会被粉碎。

为了区块交易，每一位中介用户uj都要为每一项交易payi观察一个独立选择的标识Txidij。因此，攻击者就不能把(Txid11,Txid21)对（即U1的表象）与(Txid13,Txid23)对（即U3的表象)联系起来。接下来，对于任何节点发出的支付操作，假设是S1，对手观察到的可能的接收者集是{R1,R2}。

然而，当并行交易在非区块中被解决的时候，对手观察到pay1的就是Txid11=Txid13了。因此，对手能够很好的提取出，S1发起的交易的唯一可能接收者是R1。

* 1. **Rayo：我们的构建**

**建设区块。**我们要求的是像4.1和4.2中所描述的建设区块。唯一的区别就是两个用户之间的通道条件现在被定义为channel-state := (cur(ui ,uj)[], Q(ui ,uj)[],cap(ui ,uj))，其中，cur代表了一个正在使用（部分）交易通道可用容量的交易的阵列；Q代表等待交易通道的足够可用空间的交易的阵列，而cap代表当前的交易通道的可用价值容量。

**操作。**开放通道和关闭通道保持像4.3中描述的那样。然而，这个支付操作必须扩张来保证非区块交易。我们已经在图7图8的蓝色伪代码中概括了另外的行为。

接下来，我们通俗地概括这些支付操作要求的另外的行为。简言之，当一项交易到达路径上的一个中介用户是，多个事件可以被引发。最简单的事件就是当相应的交易通道还未饱和时（即有足够的可用空间用于交易的成功进行）。用户接受交易并在cur中以正在进行的形式简单地储存它的信息。

某些更加有趣的事件会在交易通道饱和时进行，这意味着（可能多个）交易已经通过了交易通道。在这种情况下，最简单的解决办法就是中止新的交易，但是这会导致死锁的情况。然而，我们通过影响交易标识的总数的方式保证死锁不发生：如果新的交易标识（Txid）比当前进行的任何一项交易高（即包含在cur[]中），那么Txid标识的交易就会被储存在Q中。在这个行为中，如果任何一个当前进行的交易被中止，队伍里的交易(Txid∗)能够从Q中恢复并向接收者重新发送信息。另一方面，如果Txid比当前正在进行的每一个标识都低，那么这项Txid标识的交易就被直接中止，因为支付通道网络中，在有更高标识的并行交易存在下，它不可能完成。

* 1. **分析和系统讨论**

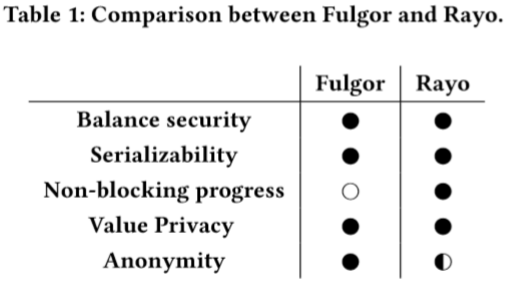
**安全和隐私分析。**接下来，我们陈述在解决非区块行为时Rayo中的安全和隐私结果。我们在(Fanon , FB)-hybrid模型中证明我们的结果。也就是说，定理5.2适用与任何UC-secure中Fanon和FB的实现（在附录A中进行了解释）。

定理5.2（UC-SECURITY）。令H:{0,1}∗→{0,1}λ为一个任意预测的哈希功能，并令（P，V）为零知识证明系统，然后是图10(Fanon , FB)-hybrid模型中描述的理想功能F的Rayo UC-realizes。

**系统讨论。**Rayo与比特币兼容，一般可以适用于支付通道网络，且支持类似于Fulgor的双向交易通道。另外，Rayo协议提供了非区块过程。具体的，Rayo保证了一些交易在每一次执行中成功地终止。直观地来看，这是因为任何两个矛盾的交易可以必要地通过他们的各自的独特标识来排序：有最高标识的决定性的被鉴定并成功完成，而优先级低的则被中止。

* 1. **Fulgor相对Rayo**

在这项工作中，我们取了这两个协议展示的交易操作的典型。如表1所示，这两个协议都保证了必要的安全和财产正确性，如结算安全和系列性。通过设计，Rayo成为唯一一个能保证非区块过程的协议。最终，考虑到隐私，我们的目标是达到尽可能的隐私。然而，尽管两个协议都有对价格隐私的保证，我们展示了非区块进程和较强的匿名机制。因此，Fulgor的成就在强匿名，而Rayo的成就在非区块进程，代价是较弱的匿名保证。但我们仍然要指出Rayo只在没有一个中介节点有危害的情况下提供关联匿名。具体的，Rayo提供了这个（较弱的）隐私保证是因为它仍然像Fulgor那样用的是多节点HTLC。



1. **绩效分析**

在这个部分中，我们首先评估Fulgor的绩效。然后再描述Rayo的开支。

我们已经在Python中开发了一个概念型的证明履行机制，我们将其与Ind的API联系起来，这是最近闪电网络发行的履行机制。我们用listchannels来提取一个开放通道的当前容量，用listpeers来从网络中其它用户提取公共密钥，再用getinfo来提取用户自己的公共密钥。我们已经用SHA-256例示了哈希功能，并且已经用以Python为基础的ZK-Boo[63]履行机制施行了多节点HTLC，以此创造零知识证明。我们设置了ZK-Boo来用SHA-256，136圈来到达完整的2-80错误证明和[69]中那样的32字节证明。

**执行层级优化。**在协议的说明书中，我们已经假设了发送者与各个中介用户创造了不同的匿名传输通道。然而，在我们的执行中，我们用Sphinx在发送者和接收者间创造单个匿名传输通道，其中的中介节点就是传输路径上的中介用户。Sphinx允许发送被要求的交易信息给每个中介用户，同时把发交给通道中国其他用户的信息模糊化，并用填塞转运信息的方式掩饰路径的实际长度。这项优化在比特币社区中已经被讨论，且在lnd[9]最近的发行中被执行。

**试验台。**我们已经模拟了五个用户的实验，创造了直线结构的交易通道：用户i只能通过用户i-1和i+1来激活支付通道，而用户4是支付操作的接收者。我们的每一个用户所用的都是分离的运行因特尔酷睿i7 3.1GHz进程和2GB RAM内存的虚拟机。这些机器通过平均延迟111.5毫秒的当地网络联结起来。在我们的实验中，我们假设每一位用户都已经开启了相应的交易通道并得到支付通道网络中国每一位用户的公共确认密钥。因为这是一个一次性设置操作，我们在实验中不考虑这个问题。

**绩效。**我们首先在lnd软件中执行可用的交易通道，这个软件用了以HTLC为基础的交易，这是因为交易通道中的条件更新合同。我们观察到有5个用户的（非隐私）支付操作需要609ms，Fulgor需要花费同样的时间。另外，Sdr必须执行SetupHTLC(n+1)协议，以此增加计算时间，另外，Sdr必须发送额外的和多节点HTLC合同相一致的信息（即(xi,yi,yi+1,πi)）给每一位中介用户，这帮助增加了传输的复杂度。

发送者需要309ms来计算每一个中介用户的πi证明，其中每一项证明都有1.65MB的大小，最后，每个中介用户还需要130ms来核实πi。我们关注零知识证明，因为它们是最贵的操作。

因此，总共的计算时间开销是1.32秒（lnd支付和多节点HTLC），而总共的传输开销少于5MB（每一位中介用户3项零知识证明加小规模价格(xi,yi,yi+1)元组）。我们观察到之前的提议[69]需要花费大概10秒的时间而仅仅计算了单个零知识证明，比较后发现，Fulgor中的支付操作只要求少于2秒的计算时间，整个交易通道上用户间的传输大小也没有超过5MB，这促进了Fulgor的运行。

**可伸缩性。**为了测试Fulgor中支付操纵的可伸缩性，我们已经研究了交易中每一轮（即发送者、接收者、中介用户）所选哟的运行时间和传输消耗。在这里，我们考虑Sphinx要求发射转运的信息以达到最大的路径长度。当实践中缺少普遍的支付通道网络的时候，我们在测试中把路径长度设置成10，就如相似的交易网络如Ripple信用网络[49]被建议的那样。

考虑到计算时间，发送者要花3.09秒来为每一位中介用户创造πi。然而，如果πi在有当前的多核系统优势的平行状态下，这项计算时间就能被改进。每一个中介用户只花费130ms，因为他们只需与后一位用户和前一位用户核实交易通道的合同。最后，接收者不需要几毫秒就能完成操作，因为她只需核实所给的价格是否正确的给出的哈希价值的原像。

考虑到传输的总开销，发送者必须创造一个有10项知识证明的信息和另外一些与中介交易通道合同相联系的极少的字节。所以，发送者总共大概要发送17MB。因为Sphinx要求在每一个节点填充信息来保证匿名，每一个中介用户都要发送一个相同大小的信息。

总的来说，这些结果说明即使是用未优化的履行，有着10个中介用户的交易也只花费少于5秒的时间且在每一位中介用户处总共只占用17MB。因此，Fulgor引发了一个相关的小的总开销，同时让支付通道网络中任何两位用户之间都能交易，并有可能被配置为有着增长用户的操作交易的支付通道网络，甚至在短短几秒内经过10位中介用户，这个结果与其他隐私保护交易系统[49，54]一致。

**非区块交易（Rayo）。**已经给出了他们定义上的相似性，Fulgor的绩效评估转结到Rayo中。另外，非区块交易的经营要求中介用户保持当前进行交易列（cur）和等待有可用容量以促进交易前进的队列（Q）这些数据结构的管理要求相当小的计算总量。另外，在这个数据结构中以Rayo的规格为依据被储存的信息数量在路线的长度上是清楚的直线型。具体的说，涉及k长度路线的交易（k ∈ N）导致了O(c · k)的信息复杂性，其中c与全部的并行复杂交易相关。

1. **相关工作**

交易通道第一次是被比特币社区[2]所介绍，而从那以后，许多伸展已经被计划了。德克尔（Decker）和沃腾赫福（Wattenhofer）[32]概括了双向交易通道[32]，Lind等人影响了组件不受比特币同步阻碍的时3用支付通道.然而，这些工作关注的是单个交易通道，它们为支付通道网络提供的扩张支持仍然是一个公开的挑战。

坦布尔比特（TumbleBit）[41]和波特（Bolt）[40]提出链下通道基础上的交易的同时坦布尔比特（TumbleBit）达到了发送者/接收者匿名，且波特（Bolt）达成了交易匿名。然而，这些途径在单节点交易中是受限制的，而且怎样把它们延伸到一般的多节点支付通道网络还不明确，也提供了私人的利益概念，就像Fulgor和Rayo所实现的那样。

闪电网络[60]已经以比特币中支付通道网络最杰出的提议的形式浮现出来。另外的支付通道网络比如比特币的雷电[19]和Eclair[10]以及Ethereum的Raiden[13]正被计划为闪电网络的微小修正。尽管它们的HTLC使用在每一项交易中都泄露一定的标识，因此降低了我们在这项工作中所说的匿名保证。此外，当前的计划缺少并行交易的非区块办法。而Fulgor和Rayo则依赖于多节点HTLC来克服与HTLC的可关联性问题，它们提供了非区块程序和匿名之间的交易。

最近的工作[49,54]计划了信用网络的隐私阐释，信用网络是一个类似于支付通道网络的支持多节点交易的系统。此外，隐私保护协议被概括为中心化[54]和分散化相结合的信用网络[49]。但是，信用网络和支付通道网络的不同在于它们不要求保证与潜在的区块链对应的责任。这个要求降低了设计一个支付通道网络的可用密码操作系列。尽管如此，Fulgor和Rayo提供了相似的隐私保证，甚至类似于在这些限制下的信用网络。

米勒（Miller）等人为交易通道计划了一个结构来减少资金被锁在中介支付通道中的时间（即并行消耗），这是一个有趣问题，但和我们的工作正交。此外，他们正式化了他们的多节点交易结构为理想功能。然而，他们关注的是并行消耗而不讨论隐私保证，因此并行交易只在区块中解决了，他们的结构依赖于Ethereum中可用的智能合同，而这个系统与当前的比特币脚本系统并不兼容。

汤斯（Towns）提出了[69]建立在zk-SNARKS上的多种HTLC合同来避免这个一个路径上的多个交易通道的可关联问题。然而，考虑到效率问题，比特币社区还未采用这个方法。在这项工作中，我们用有着被证实的安全的正式协议来重新看待这个问题并给出一个高效的ZK-Boo基础上的实例[38]。

1. **结论**

全球共识协议所管辖的无权区块链面临这其中包括可扩展性问题，以满足不断增长的用户和交易量。克服这个挑战的一个正在开发的途径由支付通道网络组成，最近的努力起源于第一个也是最初的实现比如比特币的闪电网络[60]和Ethereum的Raiden[13]。但我们只获取了表面而使很多挑战比如流动性、网络组合、路线可扩张性、并行性或隐私问题需要从根本上研究。

在这项工作中，我们为支付通道网络中的隐私和并行奠定了基础。具体的来讲，我们正式地为支付通道网络定义了普遍的可组构性结构的两种操作模式以使支付通道参与并行交易如何解决的过程（区块相对于非区块）。我们还提供了正式的被证明的例示（Fulgor和Rayo）给每一个非区块进程和匿名间的交易。我们的评估结果暗示了那在Fulgor和Rayo中展开实践是可行的并且能调整规模来满足日益增长的用户数量。

**感谢。**我们要为他们的有用的评论感谢匿名评论员，还要感谢提供python基础上的ZK-Boo履行的伊万·普里瓦洛夫（Ivan Pryvalov）。

这项工作由因特尔/CERIAS和CNS-1719196授权的国家科技基金会分别提供了部分支持。这项研究还建立在由德国研究基金会（DFG）的基础之上，我们通过与研究中心1223和巴伐利亚州纽伦堡大学科技中心（NCT）协作。NCT是一个弗里德里克-亚力克山大-大学艾朗根-纽伦堡（FAU）和技术高等院校纽伦堡乔治·西蒙·欧姆（THN）间的合作研究。

