详解最近大热的闪电网络、雷电网络和CORDA

2017-08-31 我的微信... 阅 5277 转 13

比特币闪电网络即将正式发布，闪电网络将带来极致的交易处理能力和近乎瞬时的交易确认，远超目前的VISA系统。以太坊上的类似项目雷电网络也预计将在几个月后发布。本文剖析了它们背后的原理和技术细节，并据此对R3 Corda 的原理作出一番揣测。

朱立
上交所技术有限责任公司
lzhu@sse.com.cn

1. 闪电网络（Lightning Network）

1.1 闪电网络概述

比特币自诞生起一直存在若干技术问题：论处理能力，目前全网只有7笔每秒；论时延，是大致10分钟出一个块；论交易最终性，一般建议将等待6个块的确认视作交易最终化，大额交易则建议等待更多；论容量，目前已生成40多万个区块，约60GB数据量，且眼见的未来中只见增加不见减少。

在闪电网络出现前，虽然比特币社区也试图通过区块扩容、隔离见证等技术在一定程度上增加交易处理能力，但这些方式并不能导致交易处理能力出现数量级的改善。至于前面提及的其他技术难题，现存的PoW机制是万万动不得的，需要等待多个区块的确认也是不能触碰的底线，更麻烦的是：交易处理能力和区块链数据容量似乎是一对无可调和的矛盾。

思路决定出路，常规方法找不到出路，就逼得社区换一个思路考虑这个问题。代码性能调优的经验提示我们：优化编译、改进算法、调整数据结构等方式虽然很重要也很管用，但怎么能比得上"根本不执行"的强悍？既然在比特币区块链中优化性能如此艰难，为何不尽可能将交易放到链外执行？

倚天一出，谁与争锋。以比特币区块链为后盾，在链下实现真正的点对点微支付交易，区块链处理能力的瓶颈被彻底打破，时延、最终性、容量甚至隐私问题也迎刃而解，这就是比特币"闪电网络"（Lightning Network）的思路。因为这个原因，社区甚至认为："闪电网络"的论文（The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments）对比特币的重要性仅在中本聪的创世论文之下，排名第二。

闪电网络提供了一个可扩展的微支付通道网络。交易双方若在区块链上预先设有支付通道，就可以多次、高频、双向地通过轧差方式实现瞬间确认的微支付；双方若无直接的点对点支付通道，只要网络中存在一条连通双方的、由多个支付通道构成的支付路径，闪电网络也可以利用这条支付路径实现资金在双方之间的可靠转移。

闪电网络并不试图解决单次支付的银货对付问题，其假设是单次支付的金额足够小，即使一方违约另一方的损失也非常小，风险可以承受。因此使用时必须注意"微支付"这个前提。多少资金算"微"，显然应该根据业务而定。

1.2 闪电网络技术本质

闪电网络的关键技术有三，后后依赖于前前，依次是：RSMC，HTLC和闪电网络。技术

实现虽然复杂，但本质却很简单。

1.2.1 RSMC

闪电网络的基础是交易双方之间的双向微支付通道，RSMC（Recoverable Sequence Maturity Contract）定义了该双向微支付通道的最基本工作方式。

微支付通道中沉淀了一部分资金，通道也记录有双方对资金的分配方案。通道刚设立时，初值可能是{Alice: 0.4, Bob: 0.6}，意味着打入通道的资金共有1.0 BTC，其中Alice拥有0.4 BTC，Bob拥有0.6 BTC。通道的设立会记录在比特币区块链上。

假设稍后Bob决定向Alice支付0.1 BTC。双方在链下对最新余额分配方案{Alice:0.5, Bob:0.5} 签字认可，并签字同意作废前一版本的余额分配方案{Alice:0.4, Bob:0.6}，Alice就实际获得了0.5 BTC的控制权。

类型	冻结	Alice	Bob
无条件	1.0	0.4	0.6

变为

类型	冻结	Alice	Bob
无条件	1.0	0.5	0.5

表1 前后两个版本的余额分配方案

如果Alice暂时不需要将通道中现在属于她的0.5 BTC用作支付，她可以无需及时更新区块链上记录的通道余额分配方案，因为很可能一分钟后Alice又需要反过来向Bob支付0.1 BTC，此时他们仍然只需在链下对新的余额分配方案达成一致，并设法作废前一版本的余额分配方案就行了。

如果Alice打算终止通道并动用她的那份资金，她可以向区块链出示双方签字的余额分配方案。如果一段时间之内Bob不提出异议，区块链会终止通道并将资金按协议转入各自预先设立的提现地址。如果Bob能在这段时间内提交证据证明Alice企图使用的是一个双方已同意作废的余额分配方案，则Alice的资金将被罚没并给到Bob。

实际上，前面所说的"作废前一版本的余额分配"，正是通过构建适当的"举证"证据并结合罚没机制实现的。

为了鼓励双方尽可能久地利用通道进行交易，RSMC对主动终止通道方给予了一定的惩罚：主动提出方其资金到账将比对方晚，因此谁发起谁吃亏。这个设计虽然增加了技术复杂度，但应该说是合理的。

通道余额分配方案的本质是结算准备金。在此安排下，因为要完全控制资金交收风险，每笔交易都不能突破当前结算准备金所施限制。

1.2.2 HTLC

RSMC只支持最简单的无条件资金支付，HTLC（Hashed Timelock Contract）进一步实现了有条件的资金支付，通道余额的分配方式也因此变得更为复杂。

通过HTLC，Alice和Bob可以达成这样一个协议：协议将锁定Alice的0.1 BTC，在时刻T到来之前（T以未来的某个区块链高度表述），如果Bob能够向Alice出示一个适当的R（称为秘密），使得R的哈希值等于事先约定的值H(R)，Bob就能获得这0.1 BTC；如果直到时刻T过去Bob仍然未能提供一个正确的R，这0.1 BTC将自动解冻并归还Alice。

由于到期时间T、提款条件H(R)、支付金额、支付方向的不同，同一个通道上可以同时存在多个活动的HTLC合约，加上唯一的通过RSMC协议商定的无条件资金余额，余额分配方式会变得相当复杂。假设双方初始各存入0.5 BTC，一段时间后余额分配可能这样：

类型	冻结	Alice	Bob	附注
无条件	0.5	0.3	0.2	
有条件(HTLC)	0.1	如果Alice 在T1前能向Bob出示符合H(R1)的值：0.1，否则：0.0	如果Alice在T1前能向Bob出示符合H(R1)的值：0.0，否则: 0.1	0.1 BTC
有条件(HTLC)	0.2	如果Bob在T2前能向 Alice出示符合H(R2)的值：0.0，否则：0.2	如果Bob在T2前能向Alice出示符合H(R2)的值：0.2，否则：0.0	Alice→Bob 0.2 BTC
有条件(HTLC)	0.2	如果Alice 在T3前能向 Bob出示符合H(R3)的值：0.2，否则：0.0	如果Alice在T3前能向Bob出示符合H(R3)的值: 0.0，否则: 0.2	Bob→Alice 0.2 BTC

表2 一段时间后的余额分配方案

余额分配方案是一种快照，只能整体刷新。接上表，如果Alice下一刻决定无条件向Bob支付0.1 BTC，或者Alice在T1前向Bob出示了符合H(R1)的秘密，双方将在链下交换并共同签字认定新的快照，然后构建适当的"举证"证据，结合罚没机制作废前一版本的快照。这些动作完全不出现在区块链上。
引入HTLC后，任何一方仍然能通过在区块链上公开最终余额快照的方式终止通道。

1.2.3 闪电网络

基于HTLC可以实现终极目标"闪电网络"。

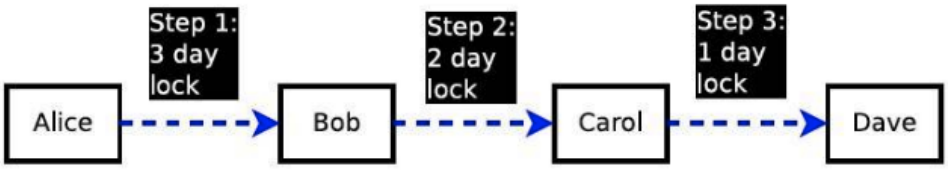


图1 闪电网络的支付路径

如上图所示，Alice想给Dave发送0.05 BTC，但Alice和Dave之间并没有微支付通道。但这没关系，Alice找到了一条经过Bob、Carol到达Dave的支付路径，该路径由Alice/Bob，Bob/Carol和Carol/Dave这样三个微支付通道串接而成。

Dave生成一个秘密R并将Hash(R)发送给Alice，Alice不需要知道R。R和Hash(R)的作用就像是古代调兵用的一对虎符。

Alice和Bob商定一个HTLC合约：只要Bob能在3天内向Alice出示哈希正确的R，Alice会支付Bob 0.052 BTC；如果Bob做不到这点，这笔钱3天后自动退还Alice。

同样地，Bob和Carol商定一个HTLC合约：只要Carol能在2天内向Bob出示哈希正确的R，Bob会支付Carol 0.051 BTC；如果Carol做不到这点，这笔钱到期自动退还Bob。

最后，Carol和Dave商定一个HTLC合约：只要Dave能在1天内向Carol出示哈希正确的R，Carol会支付Dave 0.05 BTC；如果Dave做不到这点，这笔钱到期自动退还Carol。

一切就绪后，Dave及时向Carol披露R并拿到0.05 BTC；现在Carol知道了R，她可以向Bob出示密码R并拿到0.051 BTC（差额部分的0.001 BTC成了Carol的佣金）；Bob知道R后当然会向Alice出示并拿到他的那份0.052 BTC，差额部分的0.001 BTC成了Bob的佣金。

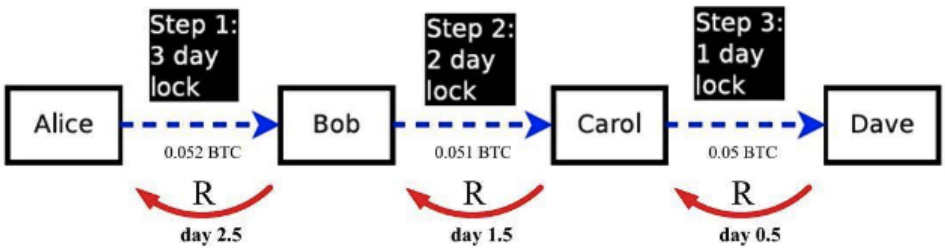


图2 闪电网络逐级提款

整个过程很容易理解。最终效果是Alice支付了0.052 BTC，Dave安全地拿到0.05 BTC，整个闪电支付网络为此收取的佣金成本是0.002 BTC。上述过程中的全部动作都发生在比特币区块链之外。

尽管闪电网络本身可以基于任何合适的传统技术构建，闪电网络的支付通道也可能逐渐向少数大型中介集中，变成若干大型中介彼此互联、普通用户直连大型中介的形式，但这种方案仍然具有传统中心化方案不可比拟的优势，因为用户现在并不需要信任中介，不需要在中介处存钱才能转移支付，资金安全受到比特币区块链的充分保护。

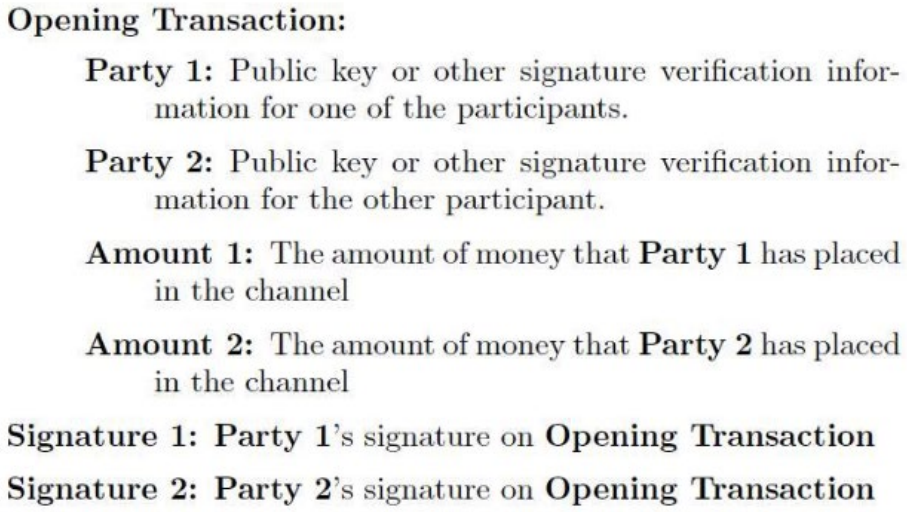
比特币闪电网络的实现方式非常复杂，不拟在此展开讲解，有兴趣的读者可以在附录一中找到详细的技术剖析。

2. 雷电网络（Raiden Network）

必须承认，虽然在区块链技术蓬勃发展的今天，比特币显得臃肿和老旧，但比特币社区仍然为区块链技术贡献着重要的思想。基于闪电网络的思路，以太坊社区也提出了自己的链下微支付通道解决方案：雷电网络（Raiden Network）。

Raiden项目源码托管在 https://github.com/raiden-network/raiden，开发语言Python，目前尚未完成，其实施原理则是基于"Universal Payment Channels"一文。当我们将以太坊作为一个侧链导入其他加密货币之后，很容易依托以太坊智能合约为各类加密货币开发微支付通道。

Raiden项目的思路直接继承自比特币闪电网络，但也有所发展。因为以太坊智能合约对报文格式没有特别的字段限制，使得Raiden得以为通道余额快照引入一个单增序号，极为轻松自然地解决了旧版本快照的识别和作废问题。
首先要在以太坊上建有一个智能合约，由此智能合约处理下文提到的OpenTransaction、UpdateTransaction等指令。


Opening Transaction:

Party 1: Public key or other signature verification information for one of the participants.

Party 2: Public key or other signature verification information for the other participant.

Amount 1: The amount of money that **Party 1** has placed in the channel

Amount 2: The amount of money that **Party 2** has placed in the channel

Signature 1: Party 1's signature on **Opening Transaction**

Signature 2: Party 2's signature on **Opening Transaction**

图3 Raiden:建立交易通道

和闪电网络一样，双方需要在以太坊区块链上开设通道并各自锁定以太。这步动作可通过向Raiden智能合约发送一条双方签名认可的报文来实现。报文中的关键信息包括：双方公钥、双方锁定资产数量、双方签名。

此后的任何支付动作都可以发生在以太坊区块链外，参与双方只需要私下传递一系列报文，其中最重要的报文是UpdateTransaction，其形式如下。

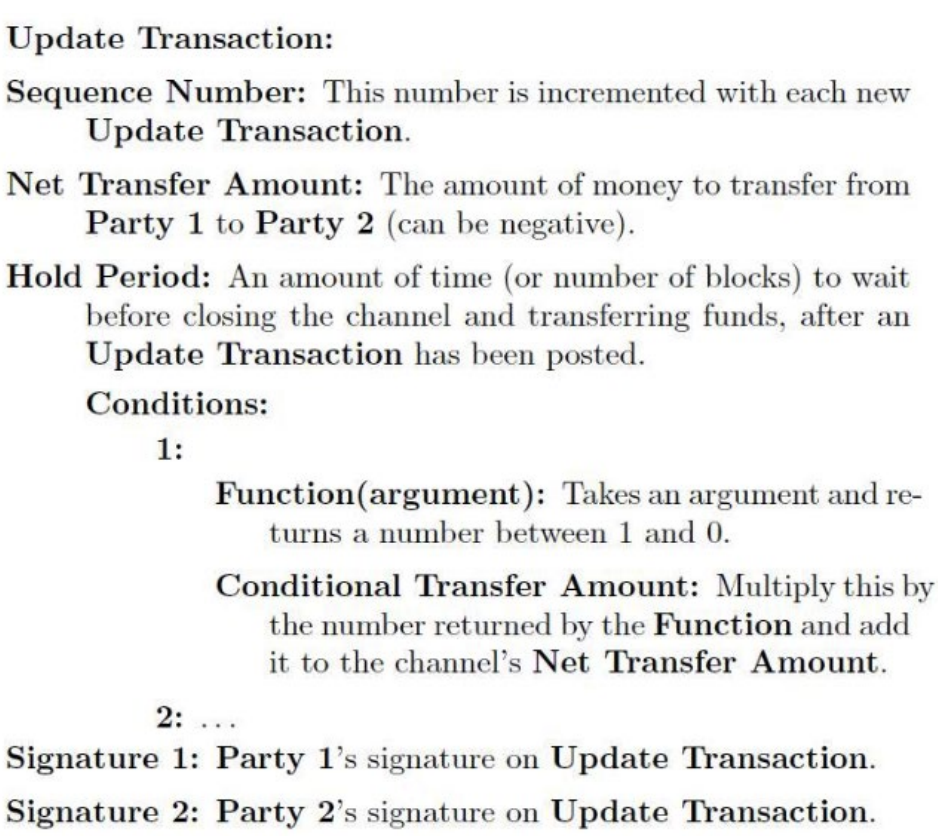


图4 Raiden:更新交易通道

此报文的内容几乎就是闪电网络的通道余额分配方案的翻版，只有几处细微的差别：

一是增加了Sequence Number字段和Hold Period字段以便识别作废的报文。A如果向区块链上合约提交一个双方签字的UpdateTransaction报文，合约将等待Hold Period时间。期间如果对手方B能够提交一个Sequence Number更高的UpdateTransaction报文，合约将没收A质押在通道中的全部资产并转移给B。如果直至等待超时B也没有异议，合约将按照报文内容在区块链上完成转移支付并关闭通道。
二是通过Net Transfer Amount隐含余额分配的方式和闪电网络略有不同，这里的方式是从建立通道时申明的Amount 1中扣减Net Transfer Amount，再将之加到Amount 2上。和直接申明余额比只是形式上的差别。
三是雷电中引入了较HTLC更为通用的"Smart Condition"。Smart Condition表现为一个可在区块链上执行的函数Function(argument)，可接受任何格式的报文为参数，执行后返回一个[0, 1]之间的数。将其返回值乘以配套的Condition Transfer Amount，再加到Net Transfer Amount上去，就完成了条件支付引发的余额调整。闪电网络中的所谓hash lock，现在成了Smart Condition的一个特例。Smart Condition能够提供远较哈希校验丰富的功能，比如可以根据某类ORACLE提供的道琼斯指数值完成衍生品合约的自动执行。

当发生争议时，只需向区块链上智能合约出示最新版本的UpdateTransaction报文，并请求智能合约对报文中的Smart Condition予以处理，就可以强制执行合约。如果没有争议，以上这一切都不会出现在以太坊区块链上，增强了隐私，又提升了性能。

其他设计思路，如通过多跳打通微支付通道、接收方提交适当的argument作为提款凭证等都和闪电网络类似。

Vitalik Buterin最近提及的State Channel技术，本质上也和这里一样，欲将区块链作为争议仲裁及强制执行的最后手段，平时则尽力避免信息在链上公开。

3. 带给Corda的启发

R3 CEV的首席技术官Richard Brown之前在博客中披露了Corda的主要特点：

没有多余的全局数据共享：只有有合法需求的参与方可以按照协议获取数据；
Corda编写和配置在企业间流转，无中心控制者；
Corda在企业间单个交易水平达成共识，而不是在系统水平上；

系统设计直接支持监管观察员节点；
交易直接由交易双方验证，而不是由一大群不相干的验证者进行；
支持多种共识机制；
记录了智能合约代码和人类语言法律文件的清晰联系；
用行业标准工具创建；
没有原始加密货币。

特征1、3、5相当值得注意。如果相关参与方只有2到3个，根据计算机科学的已知结论，他们要通过远程通信达成拜占庭容错的共识是不可能的，这也是为何目前的智能合约需要向足够数量的验证者公开的重要原因。那么Corda是怎么做到这点的?

Corda当然有可能在其核心只做了特征7，也即通过类XBRL的语言制订了一种电子化的法律文件模板，然后双方对此电子签名后就结束了。但这里的"双方电子签名"就是个两军问题。如果一方拥有了双方签名的电子合同后就不再继续，让另一方空有一份只有一方签名的电子合同怎么办?

这些疑惑的产生都很自然，但当我们见到闪电网络后，Corda的这些特征从何而来也许就不再令人费解了。

4. 总结

将交易和智能合约的执行放在链下执行，仅在必要的时候才将其在链上公开并执行，这就是闪电网络带给我们的绝佳思路。对于合适的业务场景，这种方法可以在吞吐量、确认时延、隐私保护等方面带来质的提升。

附录一 比特币闪电网络技术剖析

1. 重要说明

相比以太坊而言，为比特币增加特性受到的限制要多得多。对于以太坊开发者是小菜一碟的事情，放在比特币上很可能会成就一篇学术论文。闪电网络的技术本质并不难理解，但要将之付诸实践则相当复杂。

闪电网络的实施建立在若干BIP得以实施的基础上，比如隔离见证等等。随着社区开发工作的持续进行，障碍已被陆续扫清，闪电网络软件目前已接近正式发布状态。

闪电网络的原始论文非常难懂，很大一部分困难可能来自作者使用的图例的形式不够直观，且缺乏明确的说明。笔者将尝试使用一套新的图例，希望能够极大降低理解难度。

本文将详细剖析闪电网络所用交易结构，但不能完全代替原始论文。

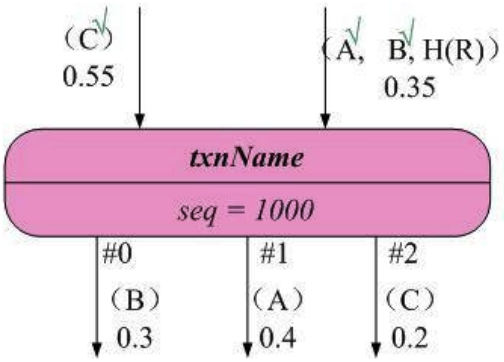


图1 比特币交易图例

图1展示了一个拥有2个输入、3个输出、保存在链下的比特币交易记录，以下逐一说明其中要素。

圆角矩形代表"交易"，用不同的底色区分交易持有者，本文一律用玫红色表示Alice，浅蓝色表示Bob。圆角矩形的边框用细实线勾勒，表示该笔交易并未公布在区块链上。

论文中每笔交易都有一个名称，虽然比特币交易结构并没有这样一个字段。我们选择将交易名

称写在圆角矩形上半部，上图中"txnName"就是这个名称。

闪电网络需要在比特币交易结构中的sequence字段和locktime字段填入适当的值，将其写在圆角矩形的下半部，如上图中的"seq = 1000"。
"0.55、0.35、0.3、0.4、0.2"都是交易输出金额。虽然"0.55和0.35"边上的箭头代表交易输入，但交易输入一定是另一交易的输出，所以这样表达仍然合理。

"0.3、0.4、0.2"边上的箭头代表交易输出。"#0, #1, #2"代表输出序号。

金额为0.3的交易输出旁边写有"（B）"，表示该笔交易输出需用B的私钥解锁。

金额为0.55的交易输入旁边写有"（C）"，意思一样，表示需动用C的私钥解锁对应交易输出。在"（C）"的右上方打有一钩（√），表示对应解锁条件已就绪。此钩颜色是绿色，表示此解锁脚本在交易拥有者拿到手时就已就绪。

"（A, B, H(R)）"代表一个特殊的解锁条件，需要同时提供A和B的私钥签名，并且需要提供一个合适的R，令其哈希值等于预设的H(R)值，才能解锁交易输出。图中A、B右上角都打有绿色的钩，表明对应解锁条件已就绪。H(R)右上角没有任何钩，表明合适的R尚未出现。

接下来我们为这笔交易提供正确的R值，并将就绪后的交易在区块链上公布，对应图例就变成这样：

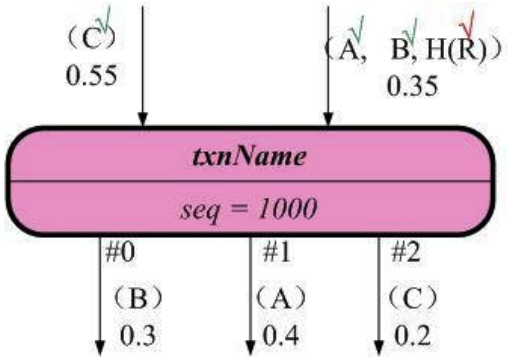


图2 解锁R并公布在区块链上的交易

注意H(R)右上方出现了红色的钩，表明对应解锁条件变为就绪。圆角矩形框的边框变成宽实线，表明这笔交易已公布在区块链上。

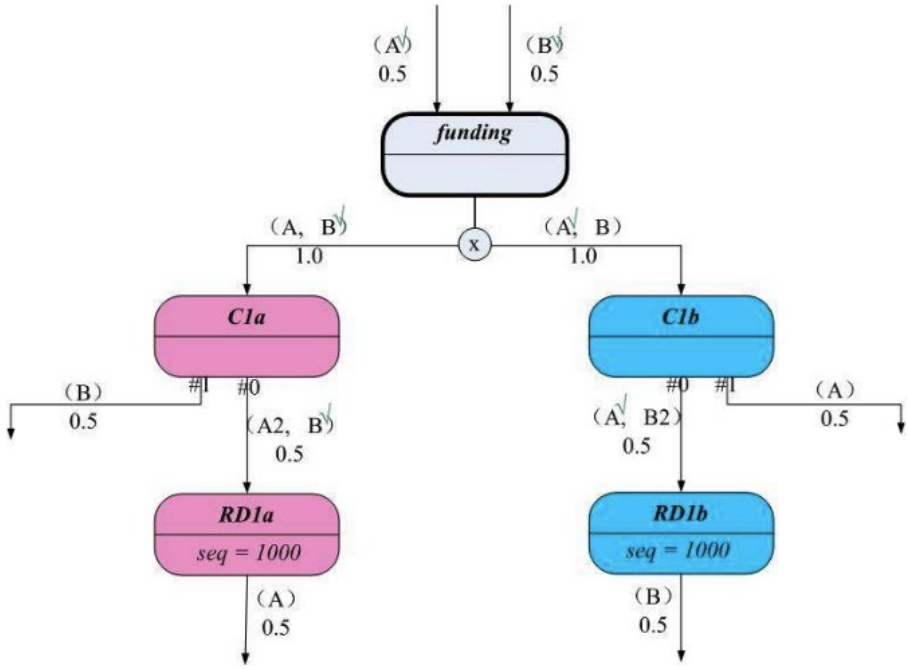


图3 互斥的交易

闪电网络允许在链下并存多个消费同一交易输出的不同交易。如果将这些交易都发布到区块链上，显然只有其中一个交易能够生效，其他交易都因为不能双花被拒绝了。上图用一个

带"X"的圆圈表达了C1a、C1b的互斥关系。

HTLC中会使用IF...ELSE...ENDIF结构的加锁脚本，就长这样子：

```
OP_IF
        OP_HASH160 <Hash160(R)> OP_EQUALVERIFY
        2 <Alice2> <Bob2> OP_CHECKMULTISIG
OP_ELSE
        2 <Alice1> <Bob1> OP_CHECKMULTISIG
OP_ENDIF
```

图4 IF...ELSE...ENDIF脚本

其中一个分支通过提供Alice2、Bob2的签名和R解锁，另一个分支只需提供Alice1、Bob2的签名就可以解锁。为特别表明此处用到了IF结构，在图例中我们会在表达互斥的带"X"圆圈旁边加注"if"，就像下图一样：

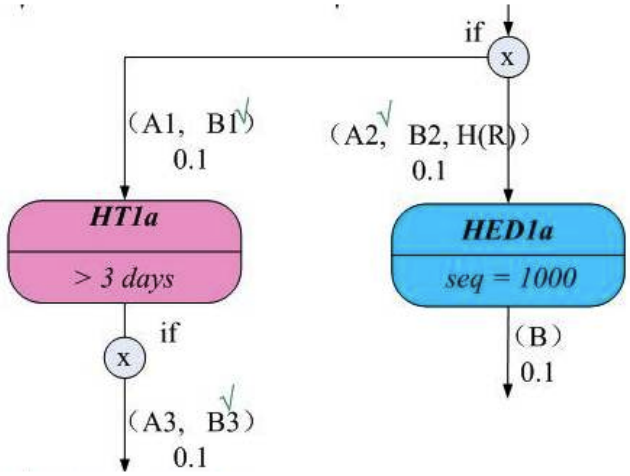


图5 if语句带来的互斥交易

2. RSMC剖析

2.1 通道建立

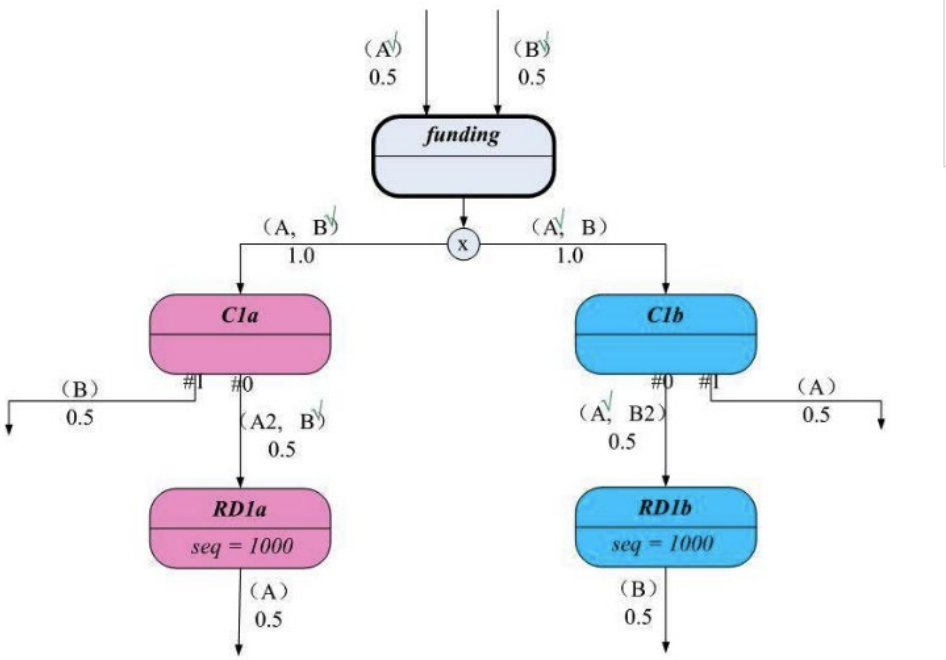


图6 通道建立

通道建立只需要双方在链下准备一套类似上图的交易结构，完成后仅将funding交易发布到区块链上（注意粗实线的边框）。上图中的A代表Alice,B代表Bob。

虽然本例中双方都向通道注资0.5 BTC，但其实各自注入多少都是可以的，不强求相等或大于0。

之所以要完全准备就绪这套交易结构后才能发布funding交易，是为了避免先发布funding交易后一方拒绝配合完成其余交易的准备活动。由于funding交易唯一的输出要求同时使用A/B双方的私钥签字才能提取，一方拒绝配合签名将导致这部分资金永久无法支取。所以合理的顺序是先准备就绪全套交易，再发布funding交易。

上图中，交易C1a虽然为Alice持有（玫红底色），但其输入解锁脚本中B已就绪，因此这条交易记录实际上是Bob准备好后给到Alice的，因为除了Bob没人能够做到这一点。C1b的输入解锁脚本中A也已就绪，说明交易记录C1b是Alice准备好后给到Bob的。

图中，交易RD1a和RD1b上都标注了"seq=1000"，这是比特币交易结构的一个最新特性，sequence字段如此设置后，交易RD1a只能在包含其父交易C1a的区块得到1000个确认后才能被收录。

2.2 单方面终止通道

通道建立后，Alice或Bob随时可以选择单方面终止通道并取回资金，发起方将受到延迟提款的惩罚。

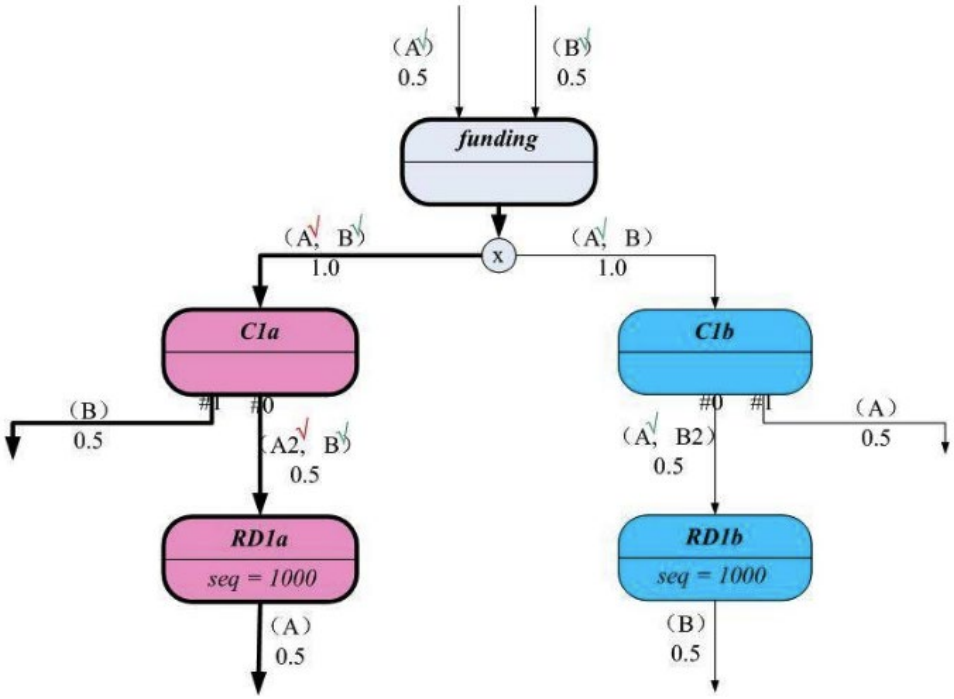


图7 Alice单方面终止通道

Alice单方面终止通道的方式如下：Alice为C1a和RD1a的输入解锁脚本用自己的私钥签名，并在区块链上发布交易C1a。由于RD1a的seq = 1000，他必须等待C1a被收录并得到1000个确认后才能发布交易RD1a，因此他需要等上10,000分钟（约7天）才能通过RD1a取回自己的款。对Bob来说，他只需要在区块链上看到C1a发布，随时可以用自己的私钥动用C1a的0号输出的资金。最终双方都得到0.5 BTC，funding交易的输出被提取一空，通道终止。

图中用粗黑有向线条表达了区块链上实际的资金流向。

2.3 微支付及旧版本废止

在双方各占0.5 BTC的基础上，Alice向Bob支付0.1 BTC，双方余额应该调整为Alice 0.4 BTC，Bob 0.6 BTC。

为此需要创建余额的新版本，然后废止余额的旧版本。由于比特币的交易由一个个离散的utxo构成，也没有多余的字段存放"版本号"，所以是迂回地通过经济手段来达到实际废止的效果。

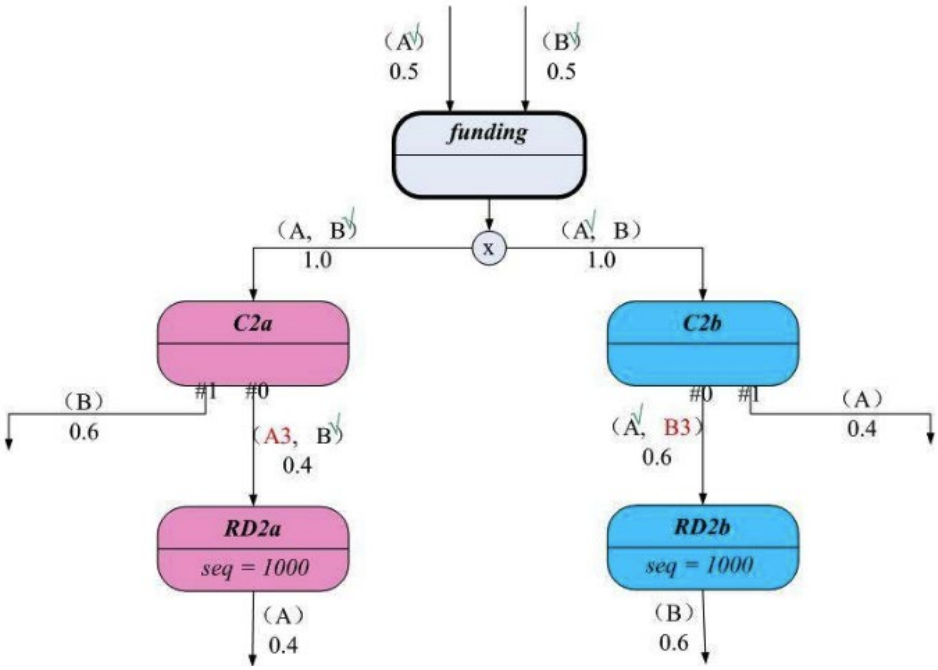


图8 微支付：创建新版本余额

创建余额的新版本很简单，双方完全不动区块链上的funding交易，在链下按上图另外创建一套反映新余额的交易。很清楚，现在Alice实际控制0.4 BTC而Bob实际控制0.6 BTC，等价于Alice支付Bob 0.1 BTC。注意为便于区分，交易名称都改变了。

作废旧版本的余额非常有技巧，方法是在旧版本交易的基础上增加几个作恶惩戒交易，效果上类似发誓："我要是拿这个旧版本去区块链上提款，你就把我的那份拿走！"，只不过这个誓言是决定可以生效的。

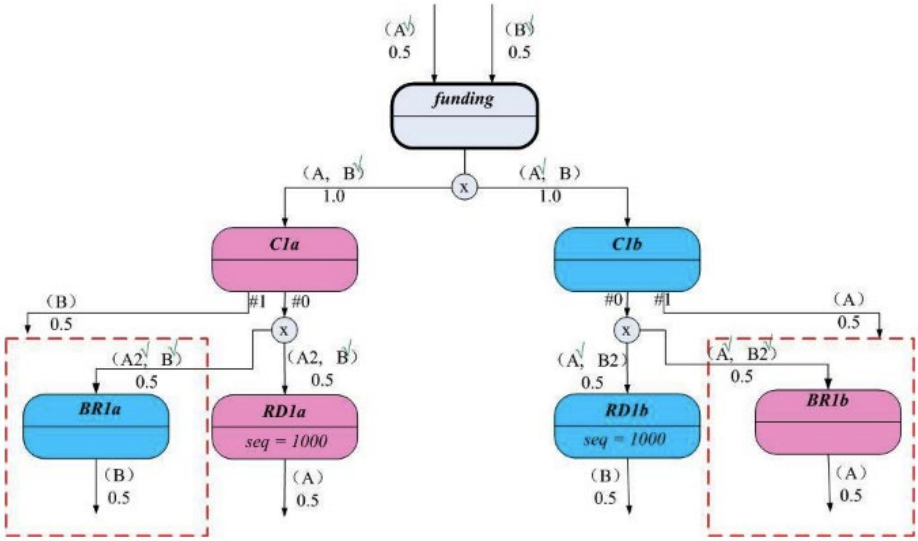


图9 微支付：作废旧版本余额

C1a, C1b, RD1a, RD1b都是旧版本余额用到的交易。作废这堆交易的方式是构造一对新的交易BR1a和BR1b，并准备就绪其输入解锁脚本所需全部签名。上图中，红色虚线框中的两笔交易是在原来基础上新增构建的。

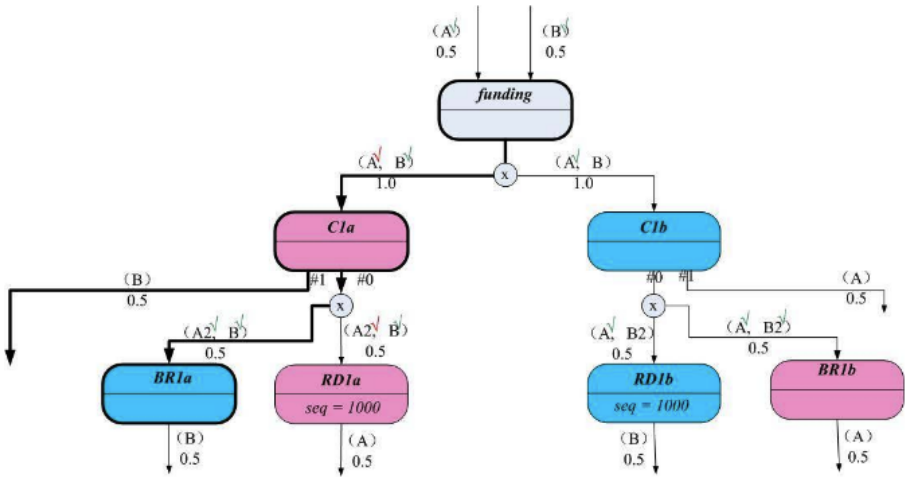


图10 微支付：惩罚措施

在图9的基础上，如果Alice希望通过在区块链上通过发布旧版本余额对应的交易来逆转刚才支付给Bob的0.1 BTC，她将受到惩罚，原理见上图。

Alice为C1a的输入解锁脚本补上自己的签名，发布到区块链上。因为交易RD1a有seq=1000的属性设定，所以Alice暂时还不能发布RD1a。但Bob将看到承诺作废的C1a被放出，为保护自身利益，Bob可以立刻在区块链上发布交易BR1a，因为BR1a的父交易已被放出，且BR1a的输入解锁脚本早已就绪，所以BR1a可以马上生效，于是Bob一共可以拿走1.0 BTC，企图作恶的Alice偷鸡不成。

正常情况下，Alice只要不在区块链上发布C1a，虽然Bob拥有输入解锁脚本完全就绪的BR1a，因为其父交易C1a并未发布，Bob也无法发布BR1a。这说明只要一方安分守己，就无需担心惩罚措施。

3. HTLC剖析

3.1 初始化HTLC

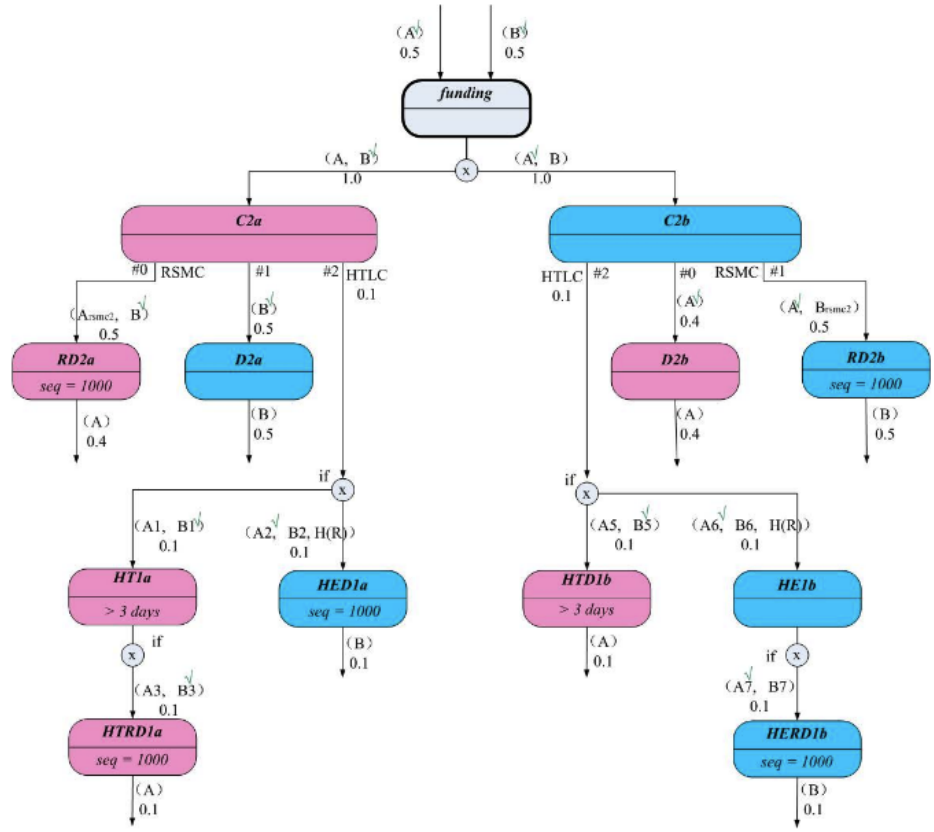


图11 HTLC的初始化

图11给出的是一个简单的HTLC示例，其所反映的通道余额划分是：有0.9 BTC以无条件余额划

分的形式在Alice和Bob之间分割，Alice占0.4 BTC，Bob占0.5 BTC。Alice向Bob有条件支付0.1 BTC，如果Bob能于3天内（实际是以区块链高度代表的未来某时）之前提供合适的R，Bob就能得到这笔钱，反之这笔钱仍然回到Alice账上。

这里的"> 3 days"是利用locktime字段的最新扩展实现的。和"seq=1000"的区别在于：locktime指定的是一个高度绝对值，而sequence指定的是相对父交易所在区块高度的相对值。

由于要在一个通道上同时反映无条件余额划分和有条件支付，所以交易结构变得相当复杂。图10中，C2a, RD2a, D2a, C2b, RD2b, D2b通过RSMC实现无条件余额划分，最下方的6笔交易专门用于HTLC支付。

3.2 条件支付的两种结果

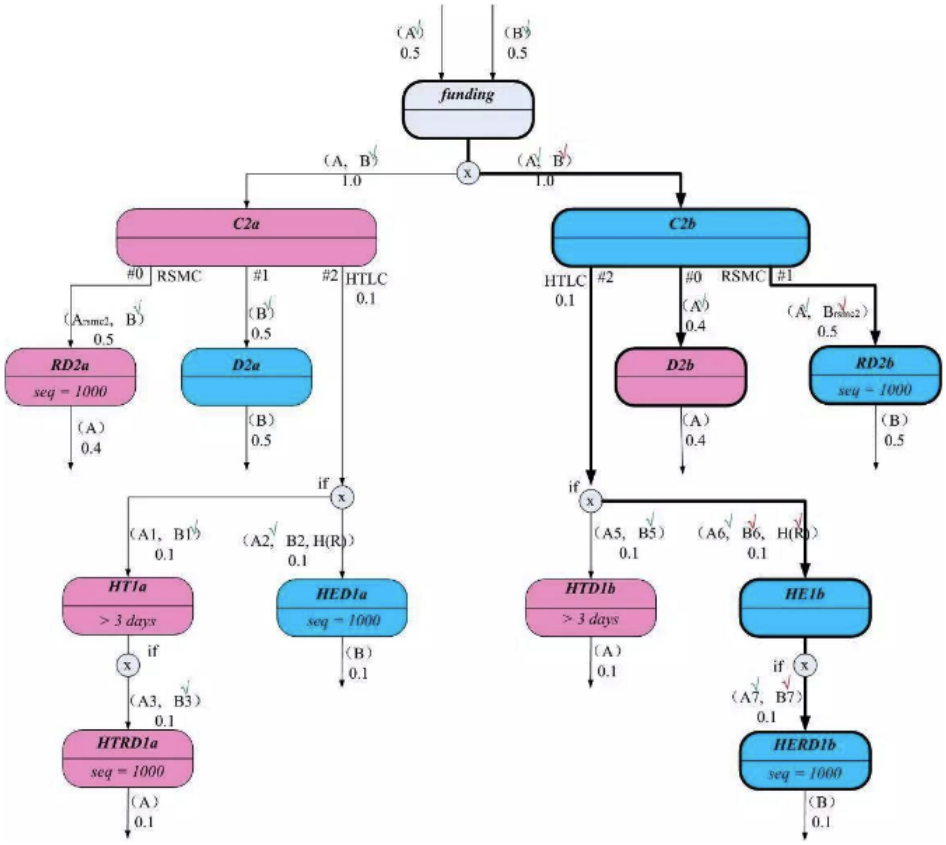


图12 HTLC：Bob及时提交R

如果Bob能够在3天内及时提交R，他可以如图11所示，准备好一系列交易的输入解锁脚本（注意图中红色的"√"）后将C2b、RD2b、HE1b及HERD1b交易发布到区块链上，拿走0.5 0.1 BTC。Alice此时只能跟着发布交易D2b拿走自己的0.4 BTC，通道终止。
也可以不终止通道，关键在于只要Bob离线告知Alice他拥有适当的R，且双方愿意达成新版本的余额划分，那么只需要新建一个Alice 0.4 BTC、Bob 0.6 BTC的新版本余额并废止旧版本，效果上就等于这0.1 BTC的条件支付已经达成。

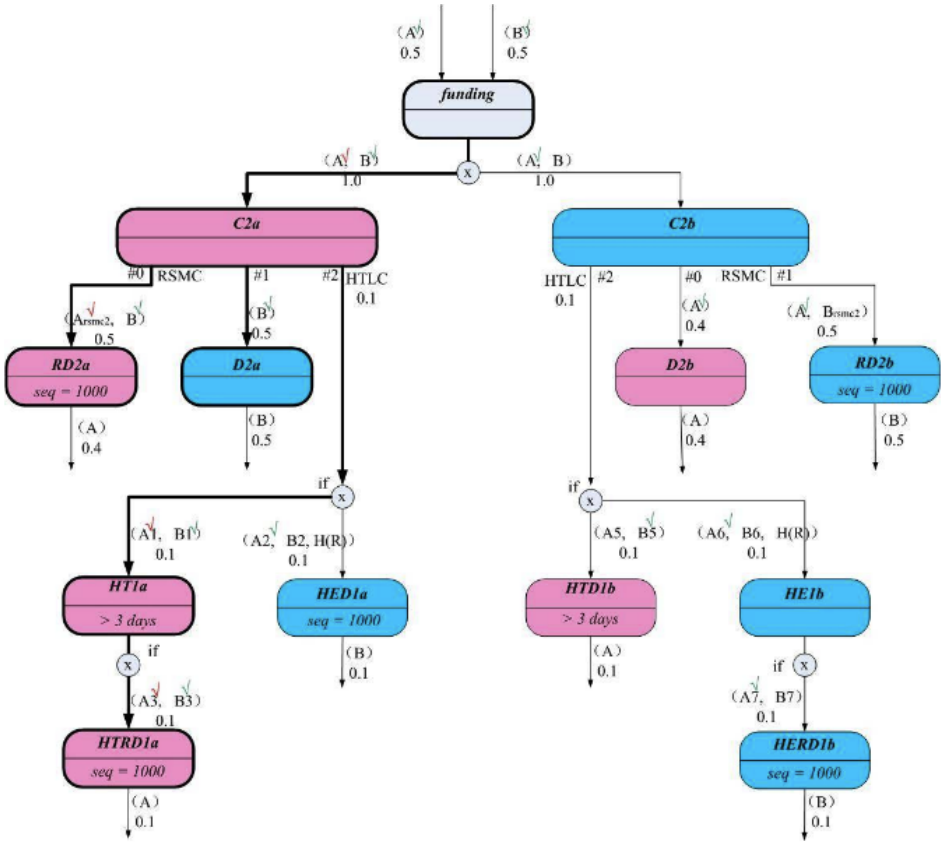


图13 HTLC: 超时退款

如果直到超时Bob仍不能提供正确的R值，Alice可以如图12所示，通过用自己的私钥准备各交易的输入解锁脚本并发布交易到区块链上，最终取回这0.1 BTC（注意图中红色的"√"），。在此方式下，最终Alice拿到0.5 BTC，Bob拿到0.5 BTC。和图11完全类似，也可以采用新建版本余额的方式，无需终止通道。

2.3 作废旧版本与违约惩罚

建立新版本余额快照后，就应该作废旧版本。和之前作废旧版本的思路类似，在通道中还包含HTLC合约的情况下，依然靠新增若干作恶惩戒交易的方式作废旧版本。

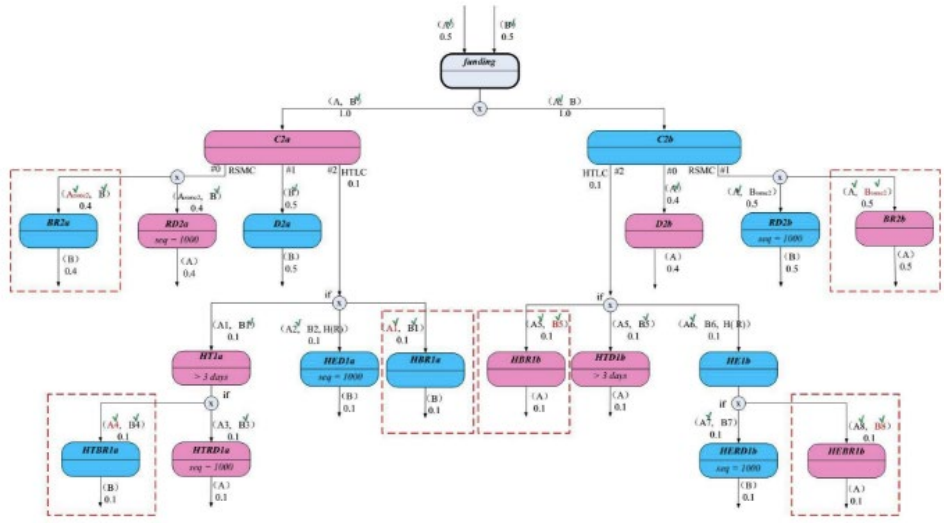


图14 作废旧版本余额

图14中用红色虚线框出的部分就是新增的"作恶惩戒交易"。

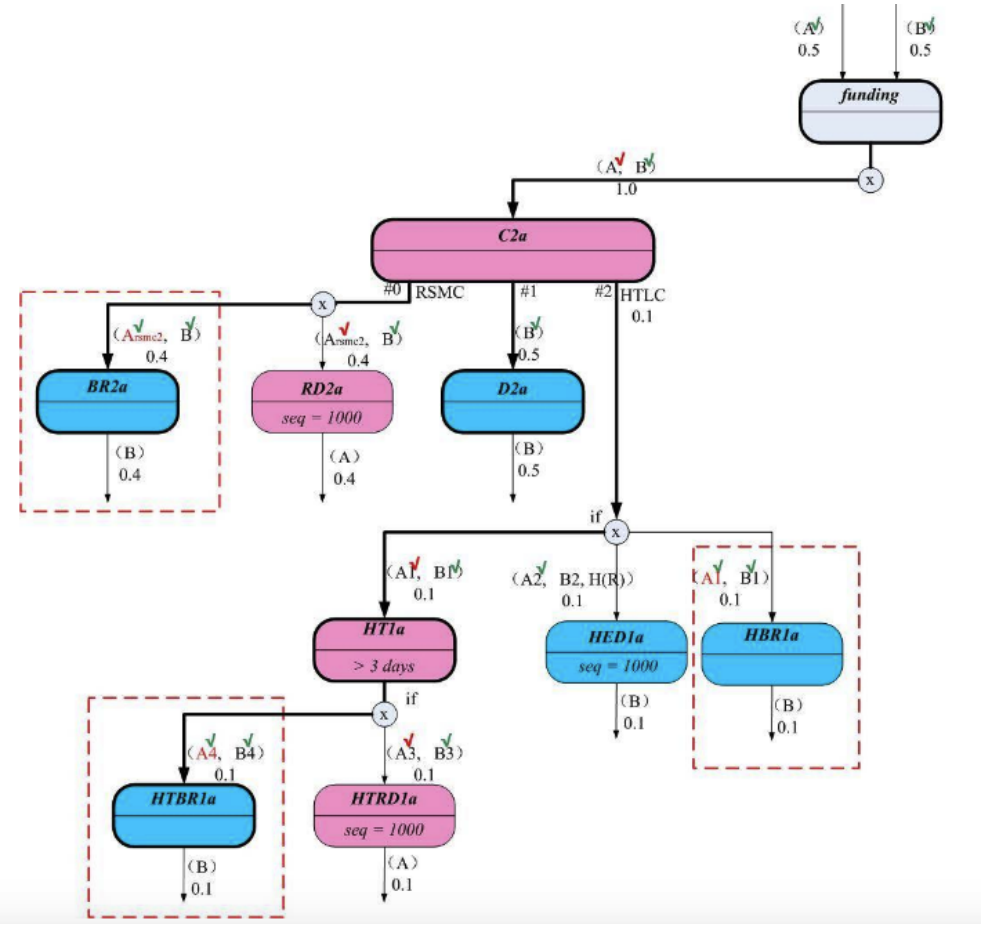


图15 惩戒交易示意

在图15中，假设HT1a交易已经超时，但以C2a为根的全部交易都已通过惩戒交易予以作废。如果此时Alice想作恶，她将C2a、RD2a、HT1a及HTRD1a的输入解锁脚本用自己的私钥准备就绪后（注意图中红"√"），将交易C2a和交易HT1a在区块链上公开。由于seq字段的限制，她不能立刻公开交易RD2a和HTRD1a，这样就使得Bob有机会发现Alice企图作恶并能够通过公布BR2a和HTBR1a交易的方式予以惩戒。发出这对交易后，通道中的全部资金将都归Bob所有。

图15中虽然没有用上惩戒交易HBR1a，但该交易并不多余。理由是：如果Alice在区块链上公布了交易C2a但故意不公布交易HT1a，倘若Bob手头没有HBR1a，也不知道秘密R，Bob将无法获得这0.1 BTC。有了惩戒交易HBR1a之后，即使Alice不公布交易HT1a，只要C2a公布，Bob也可以通过HBR1a顺利提取这0.1 BTC。

只提供HBR1a、不提供HTBR1a也是不行的。因为万一Alice选择的是解锁并公布交易HT1a，并且抢在Bob之前消费了C2a的#2输出，Bob拥有的HBR1a交易就无法生效了，而此时虽然HTRD1a交易要等上1000个确认才能公布，Bob也没有任何手段来利用这1000个块的确认时间来阻止Alice提取这0.1 BTC。

上一篇：区块链公司Cryptonomex创始人谈公司发展状况 | 巴比特

下一篇：eos的石墨烯技术是什么