利用楔入式侧链技术完善区块链

摘要 自从2009年比特币问世，并且带来了综合性计算机科学以及数字货币创新改革，人们对于分散式加密数字货币的前景产生了极大的好奇。与此同时，对比特币中已达到共识的部分进行的一些更改必须十分谨慎保守。所以，比特币相较于其他网络协议，在适应新的需要和融合新的改革这两方面，会更加的困难。

我们提出了一种新的技术——楔入式区块链，它可以使比特币和其他账簿资产在多个区块链中转移。这使用户可以利用他们的原有资产来使用一个新的、创新的分布式系统。通过重用比特币的货币流，这些系统可以更轻松地相互交互或是与比特币交互，避免了因为资金流短缺或是伴随市场波动而来的新货币的影响。自侧链成为了独立的系统以来，技术性和经济性的投资都不再被阻碍了。尽管比特币和侧链是具有双向转移性的，但是它们又是独立的：为了防止某一侧链的分布式结构的破裂（或者恶意的设计），这些损害都被完全局限于侧链本身。

这篇文章阐明了楔入式侧链和它们的执行要求，以及那些，将来会从互联互通的区块链中充分受益的工作。

**Enabling Blockchain Innovations with Pegged Sidechains**

**Abstract** Since the introduction of Bitcoin[Nak09] in 2009， and the multiple computer science and electronic cash innovations it brought， there has been great interest in the potential of decentralised cryptocurrencies. At the same time， implementation changes to the consensus critica lparts of Bitcoin must necessarily be handled very conservatively. As a result， Bitcoinhas greater difﬁculty than other Internet protocols in adapting to new demands and accommodating new innovation.

We propose a new technology， pegged sidechains， which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin’s currency， these systems can more easily interoperate with each other and with Bitcoin， avoiding the liquidity shortages and market ﬂuctuations associated with new currencies. Since sidechains are separate systems， technical and economic innovation is not hindered. Despite bidirectional transferability between Bitcoin and pegged sidechains， they are isolated: in the case of a cryptographic break （or malicious design） in a sidechain， the damage is entirely conﬁned to the sidechain itself.

This paper lays out pegged sidechains， their implementation requirements， and the work needed to fully beneﬁt from the future of interconnected blockchains.

1. 简介

David Chaum在1983年首次将数字货币作为一项研究课题提出，通过设置一个可信的中央服务器来防止双重花费[Cha83]。为了减少个人接触中央服务器而泄露隐私的风险，并且加强个人资产的可置换性，Chaum提出了盲签名，这用来创造出一个分布式手段，以防止与服务器的签名关联（这代表了钱币），这同时仍然允许服务器表现出对双重花费的防范性。

对中央服务器的需求，是数字货币的关键性弱点[Gri99]。虽然，可以通过用若干个阀值签名来代替中央服务器签名，这一形式，来使单点失败被分解成若干个小部分，但是签名的独特性和辨别性在识别过程中仍是十分重要的。这使系统仍然十分脆弱，甚至于易崩溃，因为每一个签名都可能出现问题，或者被人为一个接一个地制造出故障。

在2009年一月，Satoshi Nakamoto发布了第一个广泛使用的点对点去信任化电子货币系统，用基于工作量的共识机制取代了中央服务器的签名，用经济激励促使全局合作化运行。比特币通过聚合成区块的方法来跟踪支付，每一个区块关联有一个区块眉，用密码学的方法来指代承诺：区块的内容、时间证明、前一个区块眉。到前一个区块眉的承诺构成了区块链，或者说是指提供了一个明确交易顺序的链条。

我们可以发现，比特币的区块眉可以被看作动态成员多方签名（DMMS）的一个例子，我们将它们视作一种新类型的群体签名，具有独立的价值。比特币提供了这种签名的第一个案例，虽然并没有文字记载。一个DMMS是一个由一组签名组成的没有固定格式的数字签名。比特币的区块眉是一组DMMS，因为它们的工作量基础具有不需登记即可做出贡献的特性。此外，贡献量的衡量标准，不是每个参与者提供的门限签名，而是计算量，这可以允许参与者使用匿名身份，并且不会具有女巫攻击的风险。在这个原因的基础上，DMMS也被称为拜占庭将军问题的一个解决思路。

由于区块是连接在一起，而比特币系统的DMMS是累计在一起的：任何一个区块眉的链（或者链的一部分片段）都是第一个区块的DMMS，其计算力相当于组成它的全部DMMS之和。Nakamoto的革新关键点就是如上所述的，使用基于计算能力的DMMS签名，而不是基于知识的签名。由于签名者是证明其进行了计算工作的人，而非证明了他们仅对于特定的签名，具有特定而秘密的已知条件，所以他们被称为“矿工”。为了在区块链的记录上达到稳定的共识，经济上的激励措施以钱币的形式，被提供给了获得了报酬和津贴的矿工们，而这些钱币，只有在矿工们建立起一个有效真实的记录的情况下才是有价值的，这促使矿工们诚实地表现。因为比特币积累下来的DMMS强度与所有矿工贡献的计算力成正比，算力较少的一方是无法改变链条的。如果他们企图篡改受DMMS保护的账簿，他们就会落下进度，并且一直不发追上已达成共识的区块链。

由于矿工们没有形成一个可辨识的集体，所以他们对决定交易有效性的规则没有权利去自由裁定。因此，比特币的有效交易类型必须从一开始就确定，除非每一个网络参与者达成共识，否则无法中途添加新的有效交易类型。即使能再次达成一致，变更的部署实施也是十分困难的，因为这需要所有参与者以相同方式确认和实行新的规则，此外，还要考虑边缘情况和其他因素导致的意外的影响。

因为这些原因，比特币的目标十分简单：它是一个只支持单一数字货币转移的区块链，而不能兑换成其他任何事物。这允许了许多具体事物的简化，不过这样的简化正面临着现实世界需求的调整。尤其是，目前的创新主要围绕在以下几个方面：

1. 在可扩展性和去中心化间的取舍。例如，更大的区块可以支持更高的交易速率，其付出了增加验证方工作量的代价——中心化的风险。
2. 同样，在安全性和成本之间也存在取舍衡量。比特币历史记录中，根据同等级不可逆转的特性，存储了每一笔交易。这种方式的维护方式需要付出很大的代价，对低价值和低风险的交易来说，也未必合适（例如，所有参与者已经确定了一个共同的法律机构来处理欺骗行为）。
3. 在区块链的功能上存在更多的选择。例如，是让比特币的脚本更强大，来支持简明有用的合约，还是较少功能以便于审计。
4. 一些非货币类型的资产也可以在区块链上交易，例如欠条、其他合约和智力财产。
5. 存在一元化风险：比特币系统是由许多密码学组件构成的，其中任意一个组成部分出现问题，都会导致整体的损失。如果可以，不要用同一套算法来保护每一个比特币，这样会更加谨慎。
6. 新技术可能会带来比特币系统创立之初没有意料到的新功能。例如，利用加密累加器、环形签名Chaumian盲签名来增强对隐私的保护力量和抗审查性。
7. 即使有这样的迫切需求，但没有方法使比特币安全地升级，这意味着，只有所有参与者都协同执行，更改才能够生效。比特币的开发者们达成了一个共识，，对比特币系统的变更必须缓慢、谨慎，并且仅当社区有明确允许意向的时候才能够进行。

实际上，由于功能必须先被广泛认可后才能够被采用，这限制了参与者个人的自由和对于其钱币的自主性。体量较小的团体无法实现如专门脚本扩展这样的功能，因为他们缺少广泛的共识。

早期，比特币的这些问题的解决方法是发展可替代的区块链，又称为竞争链，除了对上述重点做出了一些修改，还共用了比特币系统的代码库。然而，想要去创建一个本质不变而独立的系统，以谋求技术的变革，这样也是存在问题的。

其中一个问题是，基础框架碎片化：由于每个竞争链都把自己的技术累积起来，所以经常会有重复性的或是缺失的工作。因此，由于采用了竞争链，可能并未去除比特币系统中一些关于安全特定领域知识的障碍，安全问题常常在不同的竞争链关系中被复制，并且它们的修复也不能解决这些问题。安全隐患一般而言无法被察觉，直到有漏洞被利用，这些问题才显现出来，而必须消耗大量资源或是请专家评审新的分布式加密系统，才可以使其被早期发现。结果，我们看到了一种动荡的、停滞不前的发展环境，大部分展示出来的项目可能在技术上是最不健全的。打个比方，想象一下在互联网上，每个网站使用自己的TCP将自定义的检验和数据包拼接算法，传播给最终用户。这不会是一个能生存且竞争链能存在的环境。

问题之二是，这样的竞争链和比特币系统一样，通常具有自己的原配加密货币，这些货币通常伴有浮动价格，它们被称为竞争币。为了使用竞争链，用户需要通过一个市场来得到这种货币，这将使他们直接面对新货币带来的高风险和波动。此外，因为有独立解决初始分配和估值的需求，与此同时还要在不良的网络效应与拥挤的市场中竞争，这既遏制了技术革新，又助长了市场的博弈。这一方面危及了这些系统的直接参与者，同时也危及到整个加密货币行业。如果这一领域在公众中留下了风险过高的印象，那么他们对加密货币会更不愿去采纳，或者有可能完全遗弃加密货币（自愿或立法上）。这说明我们希望有一个环境来让可采用交互操作的竞争链能易于创建和使用，但不要产生不必要的市场和开发碎片。此文中，我们认为这些看似矛盾的目标有可能同时实现。关键考察点是“Bitcoin”这一区块链，在概念上，是独立于bitcoin这一资产概念的：如果我们能在技术上支持区块链间资产的转移，那么可以通过简单地重复使用现有比特币的方式，研发出用户可能会采纳的新系统。

我们称这种可互操作的区块链为“楔入式侧链”，我们将在第三节中给出精准的定义，这里先列出“楔入式侧链”所需具备的属性：

1. 在不同侧链中转移的资产应该可以被他的现有持有者转移回上一个保有着，且不能是第三方（包括之前所有的持有者）。
2. 资产的交易过程中不受交易对方带来的风险：不诚实的一方没有能力去阻止转移的发生。
3. 交易应该是完全整体的，这代表了交易只能完全实现或是完全不实现。在交易记录中不应该存在交易失败的记录，或者允许非法创造的资产存在。
4. 侧链应该具有防火墙性质：一个在某侧链中创造（或移取）资产的故障，不应该在另一链条中导致出资产的创造或者移取。
5. 区块链重组必须处理得十分清晰，即使是在交易的过程中。任何破坏应该只发生在它所处的侧链上。总体上，侧链应做到完全独立，并由用户提供从其他链上得来的必要数据。侧链的验证者只有当侧链本身具有一个明显共识条件的情况下，才能被要求跟踪另外的链条。
6. 用户不应该被要求去追踪他们不经常使用的侧链。

早期“转移”钱币的解决方案是用一个可公开辨别的方式来销毁比特币，让新的区块链能检测到，以允许铸造新币[Bacl3b]，这解决了部分上面提到的问题。但这种方法还不足以满足我们的目的，因为其只允许单向转移，因此。我们提出的方案是由资产转移的交易本身提供所有者证明，以转移资产，避免让节点有跟踪发送方链的需求。从上层实现角度，当资产从一个区块链向另一个链移动时，我们在第一个区块链上创建交易，锁定资产，然后在第二个区块链上创建一笔交易，该交易的输入中包含一个确定完成的密码学证明。这些输入用某种资产类型来标记，比如创造出资产的区块链的哈希（hash）。

我们称第一个区块链为父链，每二个则简单地称为侧链。在某些模型中，两条链可对称地来处理，因此这一术语应当看成是相对的。从概念上出发，我们打算将资产从（初始）父链转移到一条侧链，可能会再转移到别的侧链，最终还能转回至父链，并保全初始资产。一般而言，我们把父链当做比特币系统，侧链是某一个从其他区块链中选取的。当然，侧链的币也可以在侧链间传递，并非只能与比特币系统进行往来：然而，因为任一最初从比特币系统移动的币都可以重新转移回去，所以不管发生了怎样的改变，它仍然是比特币。

这使前面章节提到的碎片化问题得到了解决，对于那些只想专注于技术创新的开发者来说是个好消息。此外，因为侧链是从父链中转移出原有资产而不是另铸新资产，侧链不会引起未经授权的铸币，维护资产的安全和稀缺性依靠父链来实现。

更进一步说，参与者不必再担心他们的持有物会被一个实验性竞争链锁往，因为侧链币能够用等额的父链币来赎回。这提供了一个退出机制，减少因软件无人维护而造成的损失。

从另一角度看，因为侧链仍然是一个独立于比特币系统的区块链，它们可以自由地尝试新的交易设计、信任模型、经济模型、资产保障语义，或加密特征。我们将在第5节中进一步讨论一些侧链的可能性。这一基础架构的额外好处，是对比特币系统本身进行改变不再那么迫切：用侧链来创立一个新的“改变了的比特币系统”，要比一个需要各方均达成共识并且共同实施的分叉更加好。从中期看，如果广泛认可新系统存在改进的地方，最终会明显看到，相对于比特币父链，更多的人会使用这个新系统。因为父链的规则不受任何修改，任何人都可以根据自己的时间去调整，不会有任何因共识失败所带来的风险。从长期看，侧链的成功改变，会在父链需要去做出改变的时候，为父链提供信心。

1. 设计的基本原理

“无需信任”指的是不依赖外部可信的第三方也可完成正确的操作的性质，这通常能够让所有参与方自己独立验证信息是否正确。例如，密码学签名系统中，“无需信任”是一个隐性的必要条件（如果攻击者能伪造签名，那么这个签名系统将被视为被完全破解。虽然分布式系统中一般不需如此，但比特币在系统的大部分中提供了“无信任操作”）。

“楔入式侧链”的一个主要目标是在比特币系统模型之上最小化附加的信任。难点在于币在侧链间的安全转移：接收链必须能得知发送链的币已被正确锁定。在比特币的指引下，我们提议用DMMS来解决这一问题。尽管有可能利用一个基于信任的简单方案，引入固定数量签名者来检验币的锁定状态，但有很多重要理由让我们避免这种单点故障的引入：

1. 信任个人签名者，不仅代表着期待他们做事诚实，他们还必须永远没有漏洞、永远不会泄露关键的秘密、永远不会被挟持、永远不会停止参与网络。由于数字签名是长期存在的，对任何信任的要求也必须如此。
2. 我们可以从经验中得知，即使时间跨度只有几个月，对于信任的要求也是一种危险的期待，更何况我们期望这些金融系统能延续长达几个世代时间。

在比特币系统解决单点故障前，数字货币一直没有什么吸引力，社会强烈反对引入这种脆弱的形式。2007年以来的金融危机，更加强了社会的不信任：对金融系统和其他公共机构的公共信任，也同样处于历史性的低点。

1. 双通道楔入

楔入式侧链的技术支持被称作双通道楔入。在这一部分，我们将从一些定义开始，来解释这些工作原理。

3.1定义

* 一种钱币，或者说一种资产，是一种可以被掌控者私人查看确认的数字属性。
* 一个区块，是一个由很多交易组成的集合，可以描述资产掌控过程中的各种变化。
* 一个区块链，指的是一个由许多有序的区块组成的集合，并且在这个集合中，所有用户必须（最终）达成共识。这决定了资产掌控的历史记录，并为交易提供了一种计算机科学基础上的不可删除的时间顺序记录。
* 一次重组，在某之前被接受的链条，因对手的链条提供了更多的工作量证明而被取代的情况下发生。并且失败者链条上的所有区块都会被从共识历史中删除。
* 一条侧链是一条验证其他区块链中数据的区块链。
* 双通道楔入根据一个固定的，或者说是确定的兑换汇率，在不同侧链中进行转入和转出的操作机制。
* 一个楔入式侧链是一条资产可以转出到其他链条或者转回的侧链；也就是说，一条可支持双通懂楔入的侧链。
* 简单的支付验证证明（或称为SPV证明），是一种动态成员多方签名（DMMS），发生在一条匹配于比特币系统工作量证明的区块链中。

从根本上来看，SPV证明是由一个显示出工作量证明的区块眉列表，和一个可以说明某输出发生在列表中的某一个区块的密码学证明组成的。

这使验证者，可以检查是否有一定数量的工作已经认可了某个输出的存在。当有其他证明展示了一条工作量更多的链，且生成该输出区块未包含于其中时，其他证明会使这一证明失效。使用SPV证明来确定交易历史，隐含着要信任最长的区块链，也是最长的正确区块链，在比特币系统中，这是由一个被称为SPV的客户端实现的。由于诚实的哈希算力不会为一个无效链去工作，仅当超过50%的哈希算力合作时，才能始终欺骗SPV客户端（除非客户端处于长期的女巫攻击之下，使其无法看到实际的最长链）。

另一种做法，通过获取每个区块眉，来指代区块链上未花费输出的集合，任何拥有SPV证明的人不需要“relay”，每个区块也能确定链的状态。（在比特币系统中，完全验证者第一次开始跟踪区块链时需要做这种relay。）

通过在比特币系统的区块结构中包含一些额外数据，我们可以生成比区块眉完整列表更小的证明，从而提高可扩展性。尽管如此，这样的证明还是比普通的比特币交易要大得多。

幸运的是，这些在大多数转移中并不是必须的：每条链上的货币的持有者可以直接通过原子交换来交易它们，正如我们在附录C中所说的那样。

3.2对称式双通道楔入

我们可以利用这些想法，将一个侧链SPV楔入至另一个侧链。这包含以下工作：为了将父链币转移为侧链币，父链币被发送到父链上的一个特殊输出中，该输出只能被侧链上拥有的一个SPV证明来解锁。为了在两条链上实现同步，我们需要定义两个等待周期。

1. 侧链间转移的确认期，是指币在转移至侧链之前，在父链上必须被锁定的期间。此确认期目的，是生成足够多的工作量，让下一个等待期内的拒绝服务攻击变得更艰难。典型的确认期的量级可以是一或两天。

当父链上生成了特殊输出后，用户等待确认期结束，然后在侧链上生成一个引用该输出的交易，提供出一个证明，说明它已被创建并在父链上被足够多的工作量覆盖。

确认期是一个依侧链而定的安全参数，要在跨链交易速度和安全性间做权衡。

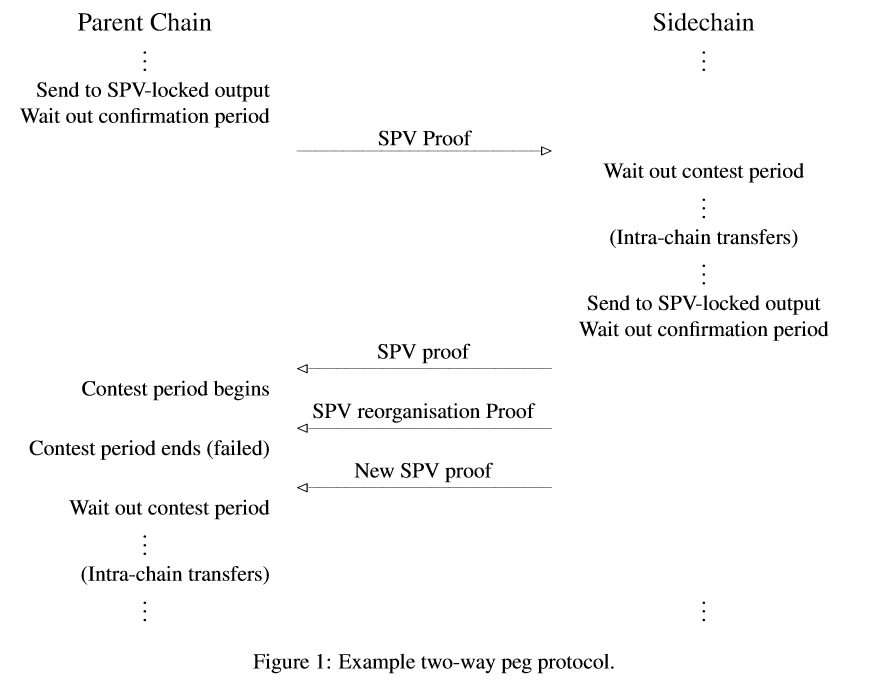
1. 接下来，用户必须等待一个竞赛期，在此期间，新转移过来的币不能在侧链上被花费，竞赛期的目的是防止重组时出现被双重花费的事件，在重组期间转走先前确定的币，在这个延迟期内的任何时刻，如果有一个新的工作证明发布出来，相应有更多累计工作量的链中没有包含那个生成已定输出的区块，那么该转换将被追加评定为失效。我们将此称为重组证明。

只要有可能，所有侧链上的用户都有能量来激发重组证明，因为承认不良证明会稀释所有币的价值。

典型的竞赛期也处于一或两天的级别上。为了避免这些延迟，只要有流动性的市场可用，用户很可能用原子交换（在附录C中有描述）进行大多数交易。

当货币被锁定在父链上时，它可以自由地在侧链中不受父链影响地转移。但是，它仍然保留了它父链货币的身份，并且只能够转移回它原来相同的链条上。

当用户想把币从侧链转移回父链上时，和之前转移的方法相同：在侧链上把货币发送至一个SPV锁定的输出上，产生一个充分的SPV证明，来说明该输出已经完成了，使用这个证明来重新释放父链上原来被锁定的那个等值的输出。整个转移过程如图所示：

由于楔入式侧链可能会从很多链中转移资产，且无法对这些链的安全性做出判定，因此，不同资产间不可相互兑换的原则是非常重要的（除非是一个展示出声明的交易）。不然，恶意用户可以通过创建一条拥有无价值资产的无价值链进行偷窃，将这样一种资产转移到一条侧链上，再使它和别的东西发生兑换。为了应对这种情况，侧链必须有效地将不同父链中的资产处置为不同的资产类型。

总之，我们提议让父链和侧链相互做数据的SPV验证，由于不能指望父链客户端能看到每条侧链，为了证明所有权，用户必须将侧链导入工作量的证明转移到父链。在对称式双通道楔入中，反向的操作也是这样的。

为了让比特币系统成为父链，需要有一个能识别和验证SPV证明的脚本扩展。最起码的要求是，这种证明需要做得足够小，以便能放进比特币系统一个交易之中。不过，这只是一个软分叉，对于不使用新功能的交易不会产生影响。

3.3非对称式双通道楔入

上节以“对称式双通道楔入”作为标题，是因为从父链向侧链的转移机制与反方向的机制是相同的：都拥有SPV安全性。

另一种方案是非对称式双通道楔入：在这样的方式下，侧链上的用户对父链都是检验者，由于所有的验证者都知道父链的状态，从父链向侧链的转移不需要SPV证明。另一方面，由于父链不知道存在侧链，所以转回到父链时需要有SPV证明。

这对安全性有所促进，现在，即使一个51%攻击者也没法错误地将币从父链转移到侧链。不过，相应的代价是迫使侧链的验证者去跟踪父链，同时也意味着发生在父链上的重组也可能导致侧链上发生重组。在这里，因为关于重组的议题会导致复杂度显著提升，所以我们不详细讨论这种可能性。

1. 缺陷

侧链为加密货币领域解决方案，系统的革新提供了十分多的机会，但同时，侧链本身也并非没有缺陷。本节我们将探讨一些潜在问题，并附以解决方案或缓解方案。

4.1复杂度

侧链在以下几个层面引入了额外的复杂度。

在网络层面，我们有了许多独立、不同步的区块链，支持相互间的转移。它们必须支持可在后期重组时被证明宣布失效的交易脚本。我们还需要软件自动检测不正当行为，以及生成并发布相关的证明。

在资产层面，简单的“一条链，一种资产”准则不复存在了：单条链可以支持任意多种的资产，甚至包括该链首次被创建时并不存在的资产，每一个这样的资产都要标记上该资产的来源链，为了保障资产的转移可以被正确地解析。

仅让区块链的基础框架能处理高级功能是不够的：管理钱包的用户界面也需要重新思考，现在，在竞争币的世界中，每条链都有自己的钱包，用来支持该链上的币发生交易，需要改写这些钱包以便支持多个链（可能带有不同的功能集合）和链间资产的转移。当然，如果为了防止使用户界面过于复杂，完全可以选择不使用某些功能。

4.2欺骗性转帐

理论上，任意深度的重组都是有可能的，这让攻击者能制造一个比发送链的竞赛期时间长的重组、在发送链撤消该半侧的转帐前。将币在侧链间完全转移结果将使接收链上币的数目与发送链上可回的领定输出的数量不对等，如果允许攻击者将币转移回初始链，他将增加他自己币的数量，让该侧链上其他用户付出损失。

在讨论如何处理这一问题前，我们应该注意到，通过简单地延长转移的竞赛期就可以使这种风险变得任意小。可以用两条链的相对哈希算力生成一个函数，以决定竞赛期的持续时间：接收链可以仅当见到一个等价于该链1天工作量的SPV证明时才解锁币，这一证明可能相当于发送链上几天的工作量证明。像这样的安全参数是特定于侧链的属性，可以针对每个侧链的应用进行优化。

不管这种事件发生的可能性有多小，很重要的一点是，不能因侧链的责任造成毁灭性故障。可以创建一个SPV证明见证这一事件，并且侧链可以接受这种证明。可以设计侧链，选下面的多种方式之一来进行处理：

* 不做应对，这样做的结果是，该侧链是一个“部分准备银行”，存储来自其他链上资产，对于微量数额，如果人们认为少于丢失的侧链币，或是有承保人承诺偿付丢失的资产，这一方式可以被接受。然而，超出一定的阈值后很可能使该侧链提现出现“银行拥挤”，最终要有某一个人承担损失。间接损害可能包括对侧链信心的普遍丧失，而父链的代价是要处理一个忽然出现的交易高峰。
* 楔入及所有相关的交易可以被回退。然而，由于币往往会散发出去，交易历史会交织在一起，即使是刚经历很短的时间就回退，后果也可能是毁灭性的。这还限制了资产的可置换性，接收者将倾向于选择历史“清白”的币（没有近期楔入的）。我们预计这种可置换性的缺失可能会导致灾难性后果。

所有币的数量可以被缩减，同时汇率不变。与新用户相比，在攻击发生前将币转移到侧链的用户会较不利。这等同于降低侧链币兑换的汇率。在这些手段基础上也可以有变化：例如，临时降低汇率，使那些在该侧链“挤兑”的人发生损失。

4.3挖矿中心化的风险

一个重要的顾虑是，引入带有矿工费的侧链是否会给矿工资源带来压力，产生比特币系统（挖矿）中心化的风险。

由于矿工们收到的报酬，来自于其所工作的各链的区块补贴及交易费，出于经济利益，他们会根据难度变化和市场价值变动，切换到价值上差不多的不同区块链，为之提供多方成员动态签名（DMMSes）。

我们的答复是，一些区块链已稍稍改进了区块眉的定义，使其中包含一个比特币系统DMMS，因而，矿工能把提交给比特币系统的DMMS同样用于一个或多个其他区块链这称为合并挖矿。因为合并挖矿允许将工作量复用到多个区块链上，矿工可以从每个他们提供了DMMSes的区块链上索取报酬。

由于矿工们要为更多的区块链提交工作，跟踪和验证全部这些链需要更多的资源。只为区块链的某一子集提交工作的矿工得到的报酬，比为所有可能的区块链都提交工作的矿工少。小规模的矿工可能无法支付为每个区块链挖矿的全部成本，因此，与较大的有组织的矿工相比，会处于劣势，后者能从更大的区块链集合中索取更多的报酬。

不过，我们注意到，矿工们可以将其所工作的任何区块链子集上的验证和交易选择分配出去。选择委托机构能使矿工免除几乎所有对额外资源的需求，或者能为仍处于验证过程的区块链提交工作。然而，这种委派有使区块链上验证和交易选择的中心化的代价，即使工作量生成本身仍是分布式的。不过，矿工们也可以选择不为仍处于验证过程的区块链工作，用自愿放弃一些报酬来提高验证过程的去中心化。

4.4软性分叉风险

比特币系统中，软性分叉是对比特币协议的一个补充，通过在设计上严格缩减合法交易或区块的集合来实现向后兼容。软性分叉的实现只需挖矿算力中的绝大多参与即可，不需要所有的完整节点都参加进来：不过，对于软性分叉出来的功能，除非所有完整节点都升级，否则参与者的安全性仅是SPV级。软性分叉已经被用于部署新功能和修复比特币系统中的安全问题十分多次了（参见[And12b]）。

按本文所述方法实现的双通道楔入仅有SPV安全性，因此，对矿工诚实性的短期依赖度高于比特币系统（参考4.2节中所述的攻击）。不过，如果双方系统的所有完整节点都相互检查，并用一个软分叉规则要求相互的合法性，那么，双向楔入的安全性可以提升至完全等同于比特币系统的水平。

这种结果这种方式的负面影响是，失去了对任何有软性分叉需要的侧链的隔离。由于隔离是使用楔入式侧链的目标之一，除非某一侧链已经几乎被普遍使用，这种结果将是不受欢迎的。不过，假设没有楔入式侧链，接下来的备选方案是直接对比特币系统硬性分叉来部署单个的更改。这会更突兀，无法提供真实的机制证明新功能成熟，还要冒比特币系统共识上的风险。

1. 应用

抛开技术基础，本节我们探讨侧链的面向用户的应用，这些应用可以有效地扩展比特币系统做它目前还不能做到的事

5.1竞争链实验

第一个应用，前面已经提及多次，就是简单地创建一条竞争链，该链上币的稀缺性由比特币系统来提供。通过利用一条不用全新货币，而是包含比特币的侧链，避免了初始分配、市场脆弱性，以及新用户障碍等麻烦的问题，新用户不需要再去找寻值得依赖的市场，或投资于挖矿硬件来获取竞争币资产。

5.1.1技术实验

由于侧链在技术上仍是完全独立的链，它们能改变比特币系统中一些功能，例如区块结构或交易链等。下面例举一些这样的功能：

* 通过修复不期望有的交易可锻性在比特币系统中只能被部分修复可以更安全地执行与链上未确认交易相关的协议。交易可锻性是比特币系统中的一个问题，会让随便一个用户以某种方式微调交易数据，尽管交易的实际内容并未发生改变，但依赖于它们的后续交易会遭到破坏。概率性支付[Cal12]就是一例可被交易可锻性破坏的协议。
* 提高支付者的隐私性，例如Monero（XMR）中使用的环签名方案，可以减少特定方的交易被审查的系统风险，保护加密货币的可置换性。Maxwell和poelstra[MP4，Poe14b]对此提出的改进能容许更高的隐私性。目前，可以用Menora币来使用环签名方案，但比特币不行：侧链将会避免这种排它性。
* 脚本扩展（例如，对彩色币[j213]的有效支持）曾被向比特币系统建议过。由于这样的扩展仅仅对小范围的用户有用，但使所有用户都要因此而应对提高了的复杂度和不易察觉的交互影响造成的风险，因而这些扩展在比特币系统中没被接受。
* 其他建议的扩展包括对新的密码学原语的支持。例如，兰波特（Lamport）签名，虽然大，但安全性可以对抗量子计算机。
* 多种用不兼容的方式扩展比特币系统的想法在[Max14]和http：//www，bitcoinninja中有说明。

因为这些变革影响的只是币的转移，而不是币的铸造，所以没必要为它们准备一种独立的货币。使用侧链，用户可以安全地、临时性地尝试这些变革。这促进了对侧链的采纳，与使用一种完全独立的竞争币相比，采用侧链时，参与者的风险更小。

5.1.2经济实验

比特币系统的奖励机制是把新币分配给矿工。这实际上使货币通胀，不过，它会按一个阶梯式时间表随时间推移而逐步下降。用这种通胀来补贴挖矿是对交易费的一个成功补充，用来保障网络安全。

在侧链上获取区块奖励的另一种方式是滞期费，这是由Freicoin首创的用于数字货币的一个想法。在滞留型加密货币中，所有未花费的输出将随时间推移而减值，减少的价值被矿工重新采集。这在证货币供给稳定的同时，还能给矿工奖励。与通货膨胀相比，这或许能更好地与用户利益保持一致，因为滞期费的损失是统一制定并即时发生的，不会像通胀那样；它还缓解了因长期未使用的“丢失”币以当前价重新回归可能给经济带来的冲击影响，在比特币系统中这是一种能预料到的风险。滞期费建立了提高货币流通速度和降低利率的激励机制，这被（例如Freicoin的拥护者和其他西尔维奥·格塞尔利息论的支持者[Ges16]）认为对社会有益。在楔入式侧链中，可以用已有价值的货币将滞期费支付给矿工。

其他与经济相关的变革，包括所需的矿工费、交易可逆性、当输出达到一定的币龄就简单地将其删除，或者是将通胀率/滞期费率楔入至侧链外的事件。所有这些变革都很难安全进行，不过，由于侧链易于创建并降低了风险，这为变革提供了必要的可行环境。

5.2资产发行

在这一点上，大多数情况下，我们认为侧链不需要自己的原生货币：所有侧链上的币最初都被锁定，直到来自其他某条侧链的资产转入将其激活。不过，侧链也可以制造自己的代替币，或是带有自己语义的资产发行。它们可以被转移给其他侧链来换取其他的资产和货币，整个过程不需要对中心方有信任，即使将来赎回时对可信方有需求。

资产发行链有很多应用，包括传统的金融工具，如股票、债券、凭证和白条等。这使得外部协议可以将所有权及转帐记录跟踪等，授权给发行所有者股份的那条侧链。发行资产链还可支持更多的创新工具，如智能财产。

这些技术还可在补充性货币[Lic01]中使用。补充性货币的例子包括：社区货币，设计目的是优先推动当地企业：企业易货协会，支持教育或老年护理之类的社会方案：限定用途的货币，在组织机构内部使用，比如大型多人游戏、客户忠诚度计划、在线社区。

一个合适的脚本扩展系统和一个资产可识别的交易，能创建出一个有用且在良好审计的组件中的交易，比如将一个出价和报价合并成一个汇兑交易，能为资产交换以及无信任占有权（FT13）这样的复杂合同创建完全无信任的点对点市场。这些合同可能会带来帮助，比如减少比特币本身的波动性。

6 未来发展

6.1哈希算力攻击抵抗能力

本文的主旨在于使用SPV证明的双通道楔入，它可被一个51%的多数方所伪造，不过也可以区块化，需要大量的哈希算力来在传输的竞赛期构建一个足够长的证明（后面这一点上要有所考量。比如，假设33%的哈希算力能使区块产出证明，那么，要想成功使用一个伪造的证明则需有67%的算力，依次类推）。

侧链中值得思考讨论的其他想法有：

* 保证合同。扣留侧链的交易费，不支付给矿工，直到他们的哈希算力至少等同于比特币系统的，比方说是，66%的第力，加密货币实现这类合同很容易只要它们最初就设计成这样，用于提高区块转移的成本。
* 时移交易费。矿工们的部分交易费要在将来的某个区块中才能收到（或分散到许多区块），使他们有动力来维持链的运作。这可以激励矿工，使其简单地收到链外交易费。传送过程中，不用常规方式，不用排队，优先传递给用户，以便及时处理的方式称为out-of-band，避免需要等待将来才能给的链内奖励。该力案的变体是让矿工收到一个牌，允许其将来挖一个低难度值的区块；这个效果是一样的，只不过更直接地激励其接收者来挖这条链。
* 滞费。区块补可以通过滞期费形式支付给矿工，以励诚实挖矿，由于被转入到比特币系统或其他侧链的数量只能与转出的数量相同，这种基金的重分配将限定在其所发生的售链之内补贴。侧链也可以发行自己独立的原生货币作为奖励，有效地形成一种竞争币。然后，这些币将有一个自由浮动的价值，结果是无法解决与竞争币相关的波动性和市场碎片等问题。
* 合签SPV证明，引入一个必须在合法SPV证明中签字的签名者，对假证明进行监察。这导致要在中心化和抗高算力攻击的安全性间接做出权衡，在这方面有很大的权衡余地：可以仅在高价值的转移中才需要签名者：仅当侧链的哈希算力过小，只相当于比特币的一个百分比时才需要他们：等等，在附录A中包含有对此类权衡的实用性的进一步讨论。
* SNARKs，密码学学术上的一个令人激动的进展是SNARK[BSCG+13]的发明。SNARK是空间效率高、可快速验证计算工作已完成的不需要知识的密码学证明。然而，因为对于大多数程序，目前它们的使用受限制，因为用当今的计算机来生成这些证明的速度太慢，且现有的构建需要一个可信设置。所以这代表系统的创建者能够制造假证明。

关于低价值或实验性侧链的一个未来想法是，起用一个可信机构，该机构的唯一任务是为SNARK方案执行一个可信设置，这样可以构建区块，证明对未花费输入集合产生了更改，不过，这是在对实现交易知识的前提完成的。这些区块还能对所有先前的区块提交完整验证，允许只验证最后建立的区，使用户的速度提升，通过根据一些先前定义的规则证明，发送例如链的合法性。这些证明还可以代替将币从一条链移至另一务链的DMMSes。

七 感谢

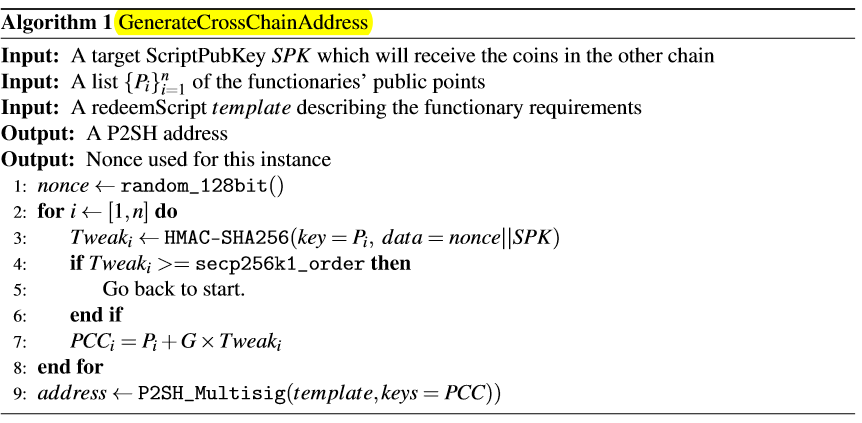
我们感谢Gavin Andresen， Corinne Dashjr， Mathias Dybvik， Daniel Folkinshteyn， Ian Grigg， Shaul Kﬁr，midnight magic，Patrick Strateman，Kat Walsh，Glenn Willen的评阅。

附录A 联合楔入

部署楔入式侧链的挑战之一是，目前比特币系统的脚本在编码SPV证明的验证规则上还不能完全表达。要用一种安全、兼容、并且径分明的方式加入所圆的表达（例如，通过用软分叉，将一个无操作no-op指令转化为一个OPSIDECHAINPROOFVERIFY指令），不过，构建共识并采用这样简单的新功能的难度很大。这些困难正是楔入式侧链产生的部分起因。我们想要的是，能有一种为比特币系统尝试未来的脚本功能，同时无需在所有地方使用的方法，。幸运的是，通过采纳一些用低信任设计目标换取的附加的安全性假设，可以在完全无许可的情况方式下进行初始尝试。

关键的考察点是，任何对比特币系统脚本的增强，都可由一个相互间不信任的工作人员组成可信联盟来评价脚本，通过签一个普通的多重签名脚本来接受，也就是说，这些工作人员充当了协议的适配器，评估那些相同规则，那些我们想让比特币系统来做，但因缺乏脚本支持而无法实现的。借助这种方法，我们能够实现一种联合的楔入。

这种方法与创建一个多重签名非链上交易系统十分相似，不过，被需要的服务器间共识达成的过程，却是由简单的问题回答观察而得到的。结果是有了一个确定性的、可审计性高的处理流程，简化了对工作人员的选择和监督。由于相似性，很多用于提高链下支付系统安全性和可信度的技术，也可以采用在联合楔入中，例如：工作人员地理位置上可以是分散的，通过托管币，或是托管创建成本高的抗协的假名身份来进行担保，在有远程证明的防幕改硬件上来实现，诸如此类tod13.对于小规的应用。系统中币的所有者自己就可以充当工作人员，从面避免了第三方信任。

一旦带有联合模入的侧链投入使用，比特币系统脚本附加的SPV验证，可被视为仅仅是一个减少系统中所信任的安全性升级，现有的侧链可以将币简单地迁移至新的验证系统中去，这种方法还开启了额外的安全选项：挖矿提供的DMMS对小型系统不是很安全。对大型的系统，联合验证会更危险，侧链可以自适应地并行使用这两种方法，或是根据明显的哈希速率来切换。考虑一个在工作人员联合体中5取3的侧链实现与比特币系统双向模入的例子，联合体有sp256k1公共点（公钥）P1、P2、P3、P4和P5以及一个赎回模板，这些对侧链中所有参与者均可见。要将币发送到一个脚本公钥SPK时，想让币在一个使用联合楔入的侧链上可用的用户可以按照下面的密钥推导方案，计算跨链P2sH[And12a] 地址。

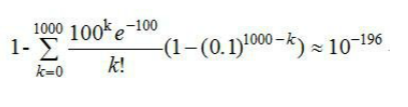
这个推导方案基于BIP32中使用的同态技术[Max11]，允许第三方导出公开的不可链接的地址。与一个支付到合同交易（GH12）的基础构建相同。产生地址后。可以将币支付到其上，通过将临时数脚本公和一个SPV证明提供给工作人员，使其可以在区块链上找到这一支付，用户随后可以在侧链上收到支付过来的币。为了帮助侧链上的第三方验证，这些数值可以包含于该侧链本身，由于币的转移是通过支付给一个标准的P2SH地址实现的，且可以支付给任何脚本公钥，所有支持支付到多重签名地址的比特币系统服务将立即能支付给，或从使用联合侧链的用户处收到支付联合模入方法需要对信任有所让步，不过不需要比特币系统作改变—仅参与者需要同意使用该方法，并且只有参与者承担使用它的代价或风险。此外，如果有人想阻止其他人使用侧链，他们是做不到的：如果联合模入在一个封闭的社区私人使用，可以让它的使用无法被检测并且无法被审查，这种方法可以允许快速部署和实验，还将允许在对比特币系统协议采用任何更改前，使社区从入式侧链中获得信心。

附录B高效SPV证明

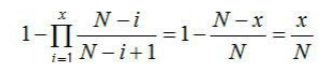
为了将币从一个侧链转移回比特币系统。我们需要加入一个证明，说明侧链币已在比特币区块链中锁定。这些证明应包含（a）一个输出已经在侧链中被创建的记录，以及（b）一个证明足够的工作量已加于该输出之上的DMMS。因为比特币系统的区块链是共享的，并被所有的参与者验证，这些证明一定不能强行在网络上有大量负担，这样输出可以很容易地紧凑记录，但让DMMS做到不是很明显的事。

紧凑型SPV安全，SPV证明的置信度可以通过将一个攻击者和诚实网络模拟为随机处理过程[MLJ14]来证明。这些随机过程有一个实用的统计特征：由于每个哈希值必须小于目标值才能合法，用一半的时间将得到小于目标值一半的值。用13的时间将得到小于目标值13的值：用1/4的时间将得到小于目标值1/4的值；以此类推。当哈希值本身不再改变当作一个区块所需的工作量时，低于必要的哈希值的部分，实际上是链上做了过多工作的统计上的证据，我们可以利用这一事实来证明仅用几个区块眉就可以达到等同的工作量[Fril4]，因而，很大程度上压缩区块眉列表并提供依旧可以证明有相同的工作量是有可能的，我们称这样一个压缩的列表为紧凑型SPV证明或压缩的DMMS。

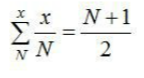
但是，在预期上，制造一个欺骗性紧凑型SPV证明与一个非紧凑型SPV证明所需的工作量是相同的，造假者成功的可能性不再随被证明的工作量而指数衰减：机会上较弱的攻击者会有更高的可能性“偶然”成功：即，早期就发现低哈希值，为了说明这一点，假设攻击者有10%的网络哈希算力，并尝试在网络能产生同样多的证明之前，创建一个1000个区块的SPV证明，按照Nak09中的公式，我们看到他成功的可能性。



作为对比，同样的攻击者在相同时间里生成一个单一的区块，且区块的价当于证明1000个区块的工作量的可能性大致为10%，这是一个很高的值，对这一问题的详细分析及其可能的解决方案超出了本文的范围，现在我们将介绍一种紧凑型SPV证明的实现，同时提供一些潜在解决方案，在阻止此类攻击的同时，仍保持证明的压缩效果。需要注意的是，我们假定了一个常量难度值。我们观察到比特币系统中的难度值，虽然不是常量，但变化得足够慢以抗拒已知的攻击Bah13，因此，我们预期根据难度调整进行校正是可以做到的实现，紧凑型SPV证明的灵感来自于跳跃表（skiplist）iPug90，一个概率性数据结构，无需再平衡即可提供对数复杂度的检索（这很有用，因为对于一种仅追加式结构，比如区块链，是无法进行二次平衡的）。我们需要比特币系统有一个改变，让每个区块眉不是仅指代它之前的一个区块眉，而是可以指明它的每个前代，为了提高空间使用效率，这些指代可以存储于一个梅克尔树中：通过在每一个区块只包含一个根哈希值，我们就可得到个对树中的每个元素的指代，其次，提取SPV证明时，允许证明者使用这些指代来跳转回某一区块，链上回指的链接不再只有一个，假使该区块眉实际证明的工作超过了仅那些跟从直接前驱链接所证明的总目标工作量，结果是一个短的DMMS证明了与原始区块链一样多的工作量这能小多少呢？假设我们尝试为一个高度为N的完整区块链生成SPV证明。为简单起见，假定该链的难度值是一个常量：即，每个区块的目标值是相同的，考虑在x个区块内找出一个可完全跳回到初始区块的足够大的证明的概率：也就是说，在区块N-x和区块N之间找到，这等于1减去我们找不到时的概率，或写成



当跳过链条上其余区块前，需要往过往方向扫描的区块数量，预期要达到



因此，如果我们想用一次跳跃来跳过整个剩余链，我们预期只需检索一半即可；用同样的方法，我们只需检索1/4即可跳过这半程，1/8即可跳过这1/4的路程。结果是预期的总证明长度是该链原始长度的对数。

一个100万区块的链，预期整条链的大小仅为10g：100000=20个区块眉，这使DMMS的大小减少至10千字节左右的范围。

然而，正如上面所观察到的情况，如果在仅实际开采了对外展示的区块眉时，攻击者就能够就可生成紧凑性证明，那么他就能在证明总工作量时以一个不能被忽略的概率也做到这一点。攻击者可以利用这样一个策略，生成无效区块，这些区块每个反向链接点指向最近的区块。当提取一个紧凑型证明时，攻击者只需每次都跟从最高权的链接即可我们可以调整方案，用以下几种方法之一来防止这种情况发生：

通过限制最大的跳跃尺寸，我们可以回归到比特币系统的性能，令攻击可能发生的概率随被证明的工作量大小呈指数衰减，利用一个常量（与最大跳跃大小成正比）因子，使预期的证明小于完整区块眉列表的大小。

通过使用一个随着工作量证明数量而增加的最大跳跃尺寸，有可能用攻击成功概率次指数衰减的代价换得次线性证明的尺寸.这能更大地节省空间，同时还令攻击者的成功概率低到足以忽略不计。

交互处理或一个切选机制可以使紧凑性证明在安全性上只有少量削减。例如，要求证明者展示随机数指定的区块眉（以及它们在区块链中的连接），使用证明的一部分作为随机数种子。当仅用一个常量因子增加证明的尺寸时，这降低了攻击的可能性

如果预期每条侧链会有很多交易，我们可以在父链中维护一个跟踪侧链末端的特殊输出，这一输出通过独立的SPV证明（可以是用上面提到的方法之一压缩的）米移动，使父链在任何时间都可以察知侧链的末端。

接下来，需要有一个总是以该未端为结束点的转移证明，可以只用一个输出查询即可验证。这保证了验证者验证的转移证明中没有“缺失的链接”，因而这些证明可以维持对数尺寸而不会使伪造的风险增加。

这使父链上的总支出与侧链的数量和长度成正比；没有这一输出，总支出还与链间的转移数量成正比。

这种讨论是没有穷尽的，优化这些取舍以及正规化安全保障超出了本文的范畴，也超出了当前进行中的工作的主题。

附录C原子交换

当某侧链可运转，就可能让用户无需使用楔入，自动在链间兑换币，实际上，现今用竞争币也可以做到，尽管独立的价格使其难于规划。这一功能很重要，因为正如我们所看到的，直接使用楔入需要相当大的交易（相应地带有高交易费）和长等待时间，与此对比，互换只需在每个网络上使用两笔交易即可完成，每个交易的大小与普通支付到地址的交易差不多。

有一个工作原理如下，其归功于Tier13的方案。

假设我们有两个成员方，A和B，在不同的区块链上持有币，假设他们在对方的链上分别有地址pk（a）和pk（b），A有一个秘密数a，那么，A可以用如下方法将币与B进行兑换：

1. 在其中一条链，A创建一笔交易，将币移动到一个输出点O（1），该输出的赎回条件限制为出示a和B的签名，或（b）A和B双方的签名，A先不宣布该交易。

A创建第二笔交易，将从O（1）返还回A，带有48小时的时间锁定，A将此交易传递给B，让B来签名。

一旦B签名了这笔锁定的退款交易，A便能够安全地宣布移动币至O（1）的那笔交易。

1. 类似地，B创建一笔交易，将币移至另一条链的一个输出O2上，该输出仅能在（a）出示a和A的签名，或（b）A和B双方的签名，时被赎回B先不宣布该交易。

B创建第二笔交易，将币从O还给B，带有一个24小时的时间锁定，B将该交易传递给A，让A来签名。

一旦A签名了这笔锁定的退款交易，B可以安全地宣布移动币到O（2）的那笔交易。

1. 因为A知道a，A能够花费O（2）中的币，A执行此操作，取得B的币。

当A执行此操作后，a暴露，B就能够花费O（1）中的币，取得A的币。