**楔入侧链的区块链革新**

Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille∗†[[1]](#footnote-1)

**摘要**：自从2009年推出比特币[Nak09]以来，它带来了多种计算机科学和电子现金创新，人们对分散式加密货币1的潜力倍感兴趣。与此同时，实施改变时对两边同样关键的共同部分必须非常保守地进行处理。因此，比特币比其他互联网协议在适应新的需求和适应新的创新方面面临着更多困难。

我们提出了一种新技术，楔入侧链，使比特币和其他账本资产能够在多个区块链之间转移。这使用户可以使用他们已经拥有的资产访问新的创新的加密货币系统。 通过重复使用比特币，这些系统可以更容易地用比特币进行相互操作，从而避免与新货币相关的流动性短缺和市场波动问题。由于侧链是分离的系统，技术和经济创新不受阻碍。 尽管比特币和楔入侧链之间有双向可转换性，但是它们是孤立的：在侧链的加密破坏（或恶意设计）的情况下，损害完全受限于侧链本身。

本文列举展示楔入侧链和它们的实现要求以及一些可以在未来从互联区块链中充分获益所需要的工作。

目录

[一.说明 3](#_Toc503114090)

[二.设计原理 6](#_Toc503114091)

[三.双向楔入技术 6](#_Toc503114092)

[3.1定义 6](#_Toc503114093)

[3.2对称的双向楔入技术 7](#_Toc503114094)

[3.3不对称的双向楔入 8](#_Toc503114095)

[四.不足 9](#_Toc503114096)

[4.1复杂性 9](#_Toc503114097)

[4.2欺诈转移 9](#_Toc503114098)

[4.3采矿集中的风险 10](#_Toc503114099)

[4.4软分叉的风险 10](#_Toc503114100)

[五.应用 11](#_Toc503114101)

[5.1竞争币实验 11](#_Toc503114102)

[5.1.1技术实验 11](#_Toc503114103)

[5.1.2经济实验 12](#_Toc503114104)

[5.2资产发行 12](#_Toc503114105)

[六.未来方向 12](#_Toc503114106)

[6.1哈希算力攻击抗性 12](#_Toc503114107)

[七.致谢 13](#_Toc503114108)

[附录A 联合楔入 14](#_Toc503114109)

[附录B高效SPV证明 15](#_Toc503114110)

[附录C 元互换(原子交换) 17](#_Toc503114111)

# 一.说明

David Chaum 在1983年将数字现金作为一个研究课题介绍给了一个可靠的中央服务器，以防止双重支出[Cha83]。为了减轻来自中央信托当事人对个人的隐私风险，以及加强真实性，Chaumin介绍了盲人识别标志，他提供了一个密码手段来防止中央服务器的识别标志（代表硬币）链接，但同时还允许中央服务器执行双重支出预防指令。 对中央服务器的要求成了数字现金的致命弱点[Gri99]。 虽然可能可以通过用多个识别标志者的门限识别标志替换中央服务器的识别标志来分发这个单一故障点，但对识别标志者是可区分和可识别的，可审计性是很重要的。 这仍然会使系统容易出现故障，因为每个识别标志者都可能失败，或者一个接一个地失败。

2009年1月，Satoshi Nakamoto发布了第一个被广泛使用的工作组不信任电子现金[Nak09]的实现，用基于工作证明[Bac02]的共识机制取代中央服务器的识别标志，同时采取经济激励措施进行合作。比特币通过将它们聚合成块来追踪付款，每块都有一个相关的块头，它以加密方式[[2]](#footnote-2)提交：块的内容，时间戳和先前的区块头。 对以前的头文件的承诺形成了一个区块链或链，它为交易提供了一个明确定义的顺序。我们观察到，比特币的区块头可以被看作是一个动态成员多方识别标志（DMMS）的例子，我们认为这是一个独立的利益，作为一种新型的组识别标志。尽管到现在为止还没有出现在文献中，比特币提供了这样一个识别标志的第一个体现，。 DMMS是由一组没有固定大小的识别标志者组成的数字识别标志。

比特币的区块头是DMMS，因为他们的工作量证明具有任何人都可以在没有注册过程的情况下贡献的属性。而且，贡献是通过计算能力来加权的，而不是每个参与方的一个门限识别标志贡献，这允许匿名成员通过恐怖攻击（当一方多次加入并且对识别标志有不成比例的输入时）。因此，DMMS也被形容为拜占庭将军问题的解决方案[AJK05]。

由于块被链接在一起，比特币的DMMS是累积的：区块头的任何链（或链段）在其第一个块中也是DMMS，其计算强度等于它组成的DMMS的总和。Nakamoto的关键创新是上述DMMS作为计算能力的识别标志，而不是知识的识别标志。因为签名者证明了计算工作，而不是像数字签名那样证明秘密知识，所以我们把他们称为矿工。 为了在区块链历史上达成稳定的共识，提供经济激励措施使矿工获得报酬和补贴，这些报酬只有在矿工形成共同有效的历史时，激励他们诚实行事时才是有价值的。由于比特币累积DMMS的实力直接与所有矿工所贡献的总计算能力相关[Poe14a]，对于少数人来说，变换链条变得不可行。 如果他们试图修改DMMS担保分类账，他们将落后，并且一直无法赶上推进一致的区块链的移动目标。

由于矿工没有形成一个可识别的集合，他们不能确定交易有效性的规则。 因此，比特币的规则必须在其历史开始时确定，并且除非得到每个网络参与者的同意，否则不能添加新的有效交易形式。即使有了这样的协议，变更也很难部署，因为这要求所有参与者以完全相同的方式执行和执行新规则，包括边缘案例和与其他特征的意外交互。

出于这个原因，比特币的目标相对来说比较简单：它是一个区块链，支持一个本地数字资产的转移，而这个资产是不可兑换的。这在实现中允许许多简化，但现实世界的需求正在挑战那些简化。 特别是，目前的创新主要集中在以下几个方面：

1. 在可扩展性和分散性之间存在权衡。 例如，较大的数据块大小将使网络支持更高的事务处理速度，但要花更多的精力在验证器上—— 集中化风险。

相似地，在安全和成本之间也有权衡。 比特币将其历史上的每笔交易都存储在同一级别的不可逆转性中。这样做的成本很低，并且可能适用于低价值或低风险的交易（例如，各方已经拥有合适的法律基础设施来处理欺诈行为）。

这些交易应该针对每笔交易进行，因为交易在价值和风险方面存在很大差异。 然而，比特币建设只支持“单一化”解决方案。

1. 区块链功能还有很多折衷。 例如，比特币的脚本可能更强大，可以使简洁和有用的合同变得简单，或者可能会减弱协助可审计性。
2. 除了可以在区块链上进行交易的货币之外，还有其他资产，如IOU和其他合约，以及智能财产[Sza97]。
3. 有单一文化风险：比特币由许多密码组件组成，其中任何一个都可能导致价值损失。 如果可能的话，谨慎的做法是不要用相同的算法来保证每一个比特币的安全。
4. 当比特币第一次被开发的时候，新技术可能使新的功能无法想象。 例如，通过使用密码累加器[Mou13]，环形签名[vS13]或Chaumian致盲[Cha83]，可以提高隐私和审查阻力。
5. 即使有迫切的需要，比特币也没有安全的升级途径，因为所有的参与者都必须协调一致地采取行动。 比特币开发商之间的共识是比特币的变化必须缓慢，谨慎地进行，只有在得到社区明确同意的情况下才能有所变化。

功能必须被广泛接受才能获得通过的事实限制了参与者的个人自由和对自己的比特币的自主权。 小组无法实现特殊功能，如特殊用途脚本扩展[jl213]，因为它们缺乏广泛的共识。

利用比特币解决这些问题的一个早期的方法就是开发替代性区块链或者竞争币区块链，它们共享比特币代码库，除了修改以外，还有共享比特币代码库。但是，通过创建独立但本质上相似的系统来实施技术变革是有问题的。

一个问题是基础架构碎片化：因为每个竞争币区块链都使用自己的技术栈，所以工作经常复制和丢失。因此，由于竞争币区块链的实施者可能无法清除比特币中安全特定领域知识的高度障碍[Poe14c]，所以安全问题通常在竞争币区块链中重复，而他们的连接则不是。 必须花费大量的资源来发现或建立专门知识来审查新型的分布式密码系统，但如果没有，安全弱点通常是不可见的，直到被利用时发现因此，我们看到了一个不稳定的，不可驾驭的环境的发展，其中最引人注目的项目可能是技术上最不可行的。 作为一个类比，设想一个互联网，每个网站都使用自己的TCP成就，向最终用户发布自定义的校验和和数据包剪切算法。 那不是一个可行的环境，目前的竞争币区块链环境也不是。

第二个问题是像比特币这样的竞争币区块链通常拥有自己的原生加密货币，或者竞争币，价格浮动。要访问竞争币区块链，用户必须使用市场来获得这种货币，使他们暴露在与新货币相关的高风险和波动性。 更进一步地，独立解决初始分配和估值问题的要求，但同时与劣势网络效应和市场竞争相悖，阻碍技术创新，但同时鼓励市场游戏。这不仅对那些直接参与这些系统的人来说是危险的，对于整个加密货币行业来说也是危险的。如果这个领域被公众认为太冒险，那么拥有可能会受到阻碍，或者加密货币可能会被完全抛弃（自愿或者是立法）。

这看起来我们渴望一个可以轻松创建和使用互操作的竞争币区块链的世界，但不会不必要地破坏市场和发展。 在本文中，我们认为有可能同时实现这些看似矛盾的目标。核心观念是，“比特币”区块链在概念上独立于“比特币”资产：如果我们有技术来支持区块链之间的资产流动，用户可以通过简单地重复使用现有的比特币来发展这一新的系统[[3]](#footnote-3)。

我们将这种可互操作的区块链称为楔入式侧链技术。 我们将在第3部分给出一个明确的定义，但是现在我们列出了以下所需的楔入式侧链属性：

1. 在侧链之间移动的资产应该能够被当前任何一个持有者移回，而没有其他人可以进行操作（包括之前的持有者）。
2. 资产应该在移动时不存在交易对手风险; 也就是说，不诚实的一方不应该有能力阻止转移的发生。
3. 转移应该是原子式的，即完全发生或根本不发生。 不应该有导致损失或允许欺诈性创造资产的失败模式。
4. 侧链应该被封锁：在一个侧链中的错误使得该链上的资产创建（或被窃）不应该导致创建或盗窃其他链上的资产。
5. 即使在转移期间，区块链重组[[4]](#footnote-4)也应该处理干净。 任何破坏都应该定位在它所在的侧链上。 一般来说，侧链应该完全独立，用户可以从其他链中提供必要的数据。 如果侧链本身是一个明确的共识规则，那么只需要对侧链的验证器进行跟踪。
6. 用户不应该被要求跟踪他们没有积极使用的侧链。

一个早期的解决方案是通过以公开可识别的方式[[5]](#footnote-5)摧毁比特币来“转让”硬币，这可以通过一个新的区块链来检测，以便创建新的硬币[Bac13b]。 这是对上述问题的部分解决方案，但是由于它只允许链之间的单向传输，所以对于我们的目的来说是不够的。

我们提出的解决方案是通过在转移交易中提供拥有证据来转移资产，避免节点追踪发送链。在高层次上，当资产从一个区块链移动到另一个区块链时，我们在锁定资产的第一个区块链上创建一个事务，然后在第二个区块链上创建一个事务，其输入包含一个加密证明，锁已经正确完成。 这些输入用资产类型标记，例如，其源于区块链的起源散列。

我们把第一块区块链称为母链，第二块简单地称为侧链。 在一些模型中，两条链都是对称的被对待，所以这个术语应该被认为是相对的。从概念上讲，我们希望将资产从（原始）母链转移到侧链，可能会转移到另一侧链，并最终返回到母链，从而保留原始资产。一般来说，我们可以将母链视为比特币，将侧链视为任何其他的区块链。 当然，侧链硬币可以在侧链之间转移，而不仅仅是来自或者去往比特币;然而，由于任何原先从比特币转出的硬币都可能被移回，它虽然如此仍然是比特币。

这让我们可以解决上一节所述的碎片化问题，这对于那些希望专注于技术创新的加密货币开发者来说是个好消息。此外，由于侧链将现有资产从母链转移而不是创造新链，因此侧链不会导致硬币的未授权创建，而是依靠母链来维护资产的安全性和稀缺性。更进一步，参与者不必担心他们的财产被锁定在一个单一的实验链中，并因为侧链硬币可以兑换成相等数量的母链硬币。 这提供了退出策略，减少了无人维护的软件带来的危害。

另一方面，由于侧链仍然是独立于比特币的区块链，因此他们可以自由地尝试新的交易设计，信任模型，经济模型，资产发行语义[[6]](#footnote-6)或密码特征。 我们将在第5节中进一步探讨侧链的许多可能性。

这种基础设施的一个额外好处是比特币本身的改变变得不那么紧迫：与其编排一个各方需要协商一致并实施的分支，不如一个新的“改变的比特币”可以作为一个侧链来创建。如果从中期来看，人们普遍认为新制度是一个改进，那么最终可能会看到比特币更为昂贵。 由于没有改变母链共识规则，每个人都可以在自己的时间切换，却没有任何与共识失败相关的风险。 那么从更长远的角度来说，侧链变化的成功将提供必要的信心来改变母链，只有当这种变化被认为是必要的。

# 二.设计原理

无信赖是不依赖于信任外部正确操作的财产，通常是通过使所有各方自行核实信息是正确的。 例如，在密码签名系统中，无信任是一个隐含的要求（攻击者可以伪造签名的签名系统将被认为是完全破坏的）。虽然这在分布式系统[[7]](#footnote-7)中并不常见，但比特币确实为其系统的大部分部分提供了可靠的操作。

楔入侧链的主要设计目标是尽量减少对比特币模型的额外信任。 困难的部分是确保侧链之间的硬币转移：接收链必须看到发送链上的硬币被正确锁定。跟随着比特币的领导，我们建议使用DMMSes来解决这个问题。 尽管有可能使用一个简单的基于信任的解决方案，包括固定签名者（见附录A）来验证硬币的锁定，但有一些重要原因去避免引入单点故障的引导：

* 信任个人签名者不仅意味着期望他们诚实行事，他们绝对不会被折衷，也绝不会泄露秘密密钥，绝不会被强迫，永不停止参与网络工作。
* 由于数字资产是长期存在的，所以任何信任要求都必须如此。 经验表明，即使是几个月的时间跨度，信任要求也是危险的预期，更不用说我们期望金融系统能够持续的世代时间跨度。
* 在比特币能够消除单点故障之前，数字货币无法获得牵引力，并且社区则强烈反对引入这样的弱点。 自2007年以来，社区不信任受到财务事件的强化。 公众对金融体系和其他公共机构的信任同样处于历史低谷。

# 三.双向楔入技术

楔入楔入式侧链的技术基础被称为双向楔入技术。 在本节中，我们从一些定义开始阐明其工作。

## 3.1定义

• 硬币或资产是数字财产，其控制器可以密码确定。

* 区块是一组描述资产控制变化的交易的一种集合。
* 区块链是一个有序的区块集合，其中的所有用户都必须（最终）达成共识。 这决定了资产控制的历史，并为交易提供了计算上不可伪造的时间顺序。
* 当一个以前被接受的区块链被拥有更多的工作证明的竞争区块链超越了，那么在客户当地就会发生重组，导致在分叉丢失一方的任何区块被删除共识历史。
* 侧链是验证来自其他区块链的数据的区块链。
* 双向楔入是指硬币以固定或其他确定性汇率在侧链和背面之间转移的机制。
* 一个楔入侧链是资产可以从其他链条进口和返回的侧链，也就是一个支持双向楔入资产的侧链。
* 一个简化的支付验证证明（或SPV证明[[8]](#footnote-8)）是一种其行为发生在与比特币类似的工作证明区块链上的DMMS。

本质上，SPV证据由（a）工作证明的分块头列表和（b）一个输出是在列表中的区块中创建的密码证明组成。这使得审计人员能够检查一定数量的工作是否存在于输出中。 这样的一个证明可能会被另一个，表明一个链的存在的，用更多的不包括产生输出的块的工作，这样一个证明废止。

使用SPV证据来确定历史，隐含地相信最长的区块链也是最长的正确区块链，是由比特币中所谓的SPV客户完成的。 只有一个与超过50％的哈希算力进行不诚实的勾结可以持续欺骗SPV客户端（除非客户端在Sybil的长期攻击下，阻止它看到实际最长的链），因为诚实的哈希算力将无助于无效链。

可选地，通过要求每个区块头提交区块链的未使用的输出集合[[9]](#footnote-9)，拥有SPV证明的任何人都可以确定链的状态，而不需要“重放”每个区块。 （在比特币中，完整的验证者在首先开始跟踪区块链时需要这样做。）

正如我们将在附录B中讨论的那样，通过在比特币的块结构中包含一些额外的数据，我们可以产生比完整区块头头列表小的证明，这将提高可扩展性。 但是，这些证据将比普通的比特币交易大得多。 幸运的是，它们对于大多数转移来说并不是必须的：每个链上的硬币持有人可以使用原子交换[Nol13]直接交换它们，如附录C所述。

## 3.2对称的双向楔入技术

我们可以用这些想法让SPV把一个侧链固定在另一个侧链上。 这工作如下：将母链硬币转换成侧链硬币，将母链硬币发送到母链上的只能通过侧链拥有的SPV证明来解锁的特殊输出位置。 要同步两条链，我们需要定义两个等待期：

1. 一个在侧链之间转换的确认期限是一个硬币在转移到侧链之前必须锁定在主链上的期限。这个确认期的目的是为了足够的工作被创造以便在下一个等待期内进行拒绝服务攻击变得更加困难。 一个典型的确认时间大概是一两天。

在母链上创建特殊输出后，用户等待确认期，然后在引用该输出的侧链上创建一个交易，提供一个证明它是在母链上充分工作的情况下创建和隐藏的SPV证明。

确认期是为了安全性而更换交叉链式传输速度每个侧链的安全参数。

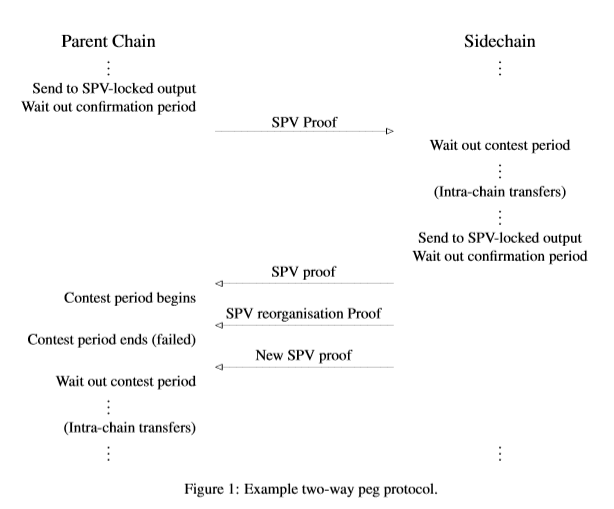
1. 用户必须等待争论时间。 这是一个重新转移的硬币不得花在侧链上的时间。 争论期间的目的是通过在重组期间转移先前锁定的硬币来防止双倍花费。

如果在这个延迟期间的任何时候，发布一个新的包含一个更多的集合工作但不包括创建被锁定的输出的块的链的证明，，则该转换被追溯无效。 我们称之为重组证明。

如果可能的话，所有的侧链用户都有动机提供重组证明，因为提交错误证据的结果是所有硬币价值的稀释。

典型的争论时间也将在一两天左右。 为了避免这些延误，只要流动性市场空闲，用户可能会使用原子互换（见附录C）进行大多数转移。

当锁定在母链上时，硬币可以无需与母链进一步互动就可在侧链内自由转移。 但是，它保留了它作为母链硬币的身份，并且只能被转移回它来的地方。当一个用户想要将硬币从侧链转移回母链时，他们做和原来的转移一样的事情：将侧链上的硬币发送给SPV锁定的输出，产生足够的SPV证明，证明完成后，使用证明可以解锁母链上相同面额的多个以前锁定的输出。整个传输过程如图1所示。



由于被楔入侧链可以从许多链条上运载资产，并且不能对这些链条的安全性作出假设，不同的资产是不可互换的（除非是明确的交易）是重要的。否则，恶意用户可能会通过创建一个无价值资产的无价值链来执行盗窃行为，将这样的资产转移到侧链，并将其交换为其他东西。 为了解决这个问题，侧链必须将母链中的单独资产作为单独的资产类型进行有效处理。

总之，我们建议让母链和侧链互相做SPV验证数据。 因为不能期望母链客户观察到每一个侧链，因此用户将侧链工作证明导入到母链中以证明拥有。 在对称的双向楔入中，反过来也是正确的。

要使用比特币作为母链，需要对脚本进行扩展以识别和验证此类SPV证据。 最少，这样的证明也需要足够紧凑以适应比特币交易。然而，这只是一个软分叉的变化[[10]](#footnote-10)，对不使用新功能的交易没有影响。

## 3.3不对称的双向楔入

前一节标题为“对称双向楔入”，因为从母链到侧链和回来的转换机制是相同的：两者都具有SPV安全性[[11]](#footnote-11)。

一个备用方案是不对称的双向楔入：这里侧链的用户是母链的完整验证者，并且从母链转移到侧链不需要SPV证明，因为所有验证者都知道母链的状态。 另一方面，母链却仍然不知道侧链，所以SPV证明需要移回。  
 这提高了安全性，从现在开始即使51％的攻击者也不能将硬币从母链错误地移动到侧链。 然而，这是以牺牲强迫侧链验证者来追踪母链，也意味着对母链进行重组可能会导致侧链重组。 在这里我们不详细探讨这种可能性，因为围绕重组的问题会导致复杂性显著扩大。

# 四.不足

尽管侧链为加密货币领域的许多问题提供了解决方案，并为比特币的革新创造了无数的机会，但它们并非没有缺点。 在本节中，我们将回顾一些潜在的问题以及解决方案或解决方法。

## 4.1复杂性

侧链在几个层面上引入了更多的复杂性。

在网络层面上，我们有多个独立的非同步区块链彼此之间支持转移。 他们必须支持交易脚本，这样可以通过后来的重组证明来使其失效。 我们还需要能够自动检测不当行为的软件，并生成和发布这些证据。

在资产层面，我们不再仅仅有“一条链，一条资产”的格言， 个别链可以支持任意多的资产，甚至连第一次创建时都不存在的资产。 这些资产中的每一个都标有从其转移来的链条，以确保其转移可以正确解开。

启用区块链基础架构来处理高级功能并不足够：用于管理钱包的用户界面需要重新考虑。 目前在竞争币世界里，每个链都有自己的钱包，支持该链的硬币交易。 这些将需要适应支持多个链（具有潜在不同的特征集）和链之间的资产转移。 当然，当界面过于复杂的时候总会有不使用某些功能的选择。

## 4.2欺诈转移

任意深度的重组在原则上是可能的，这可以允许攻击者在重组之前完全转移侧链之间的硬币，而重组时间比发送的链的争论时间长，以撤销其一半的转移。 结果将是接收链上的硬币数量与在发送链上锁定输出值的数量之间的不平衡。 如果攻击者被允许将被转移的硬币归还原始链，他将在损害他人的侧链的基础上增加他拥有的硬币的数量。

在讨论如何处理这个问题之前，我们注意到只要简单地增加转移的争论时间就可以使这个风险任意变小。 更好的是，争论期间的持续时间可以根据两条链的相对散列强度来确定：接受链可能只能解锁硬币被发送了证明一天的工作证明的价值的SPV证明，这可能相当于几天的发送链的工作证明。 像这些安全参数是特定侧链的属性，并可以为每个侧链的应用程序进行优化。

无论这个事件发生的可能性如何，重要的是侧链不会以灾难性的失败作出回应。创建一个见证这种事件的SPV证明，而且侧链可以接受这样的证明是有可能的。 他们可能被设计为以许多可能的方式之一作出反应：

* 没有反应。 其结果是，侧链是其他链中存储资产的“部分储备”。 对于认为少于丢失的侧链硬币数量的小数额，或者保险公司承诺弥补缺失资产的情况，这可能是可以接受的。然而，超出一定的门槛，可能会导致从侧链退出的“银行挤兑”，这将最终导致有人拿着这个袋子。 间接损害可能包括对侧链信心的普遍丧失，以及母链处理突然急于交易的费用。
* 楔入和所有的依赖交易可以颠倒。 然而，随着硬币的扩散和历史的混合，这种逆转的影响在短时间之后可能是灾难性的。 这也限制了互换性，因为收款人会选择具有“清洁”历史的硬币（最近没有被楔入）。 我们预计这种可替代性的丧失可能会有灾难性的后果。
* 所有硬币的数量可以减少，而汇率保持不变。 现在在攻击之前将硬币转移到侧链的用户相对于新的而言是不利的。降低侧链硬币的兑换率是相当的。

这些反应可能会有很多变化：例如，暂时降低汇率，那么那些在侧链上“跑动”的人就会覆盖那些不了解的人。

## 4.3采矿集中的风险

一个重要的问题是，引入侧链矿业费是否对矿工造成资源压力，造成比特币集中化风险。

因为矿工从他们提供的每一个环节的补贴和费用中获得补偿，在改变困难和市场价值变动之后，为不同价值的区块链提供DMMS之间的切换是符合他们经济利益的。

一个回应是，一些区块链调整了区块头的定义，这样它就包含了比特币DMMS的一部分，因此使矿工能够提供一个单一的比特币DMMS以及一个或多个其他区块链 - 这就是所谓的合并挖掘。 因为合并开采可以重复使用多个区块链，矿工可以从每个区块链中索取补偿，这些区块链可以提供DMMS。

随着矿工们提供更多区块链的工作，需要更多的资源来跟踪和验证所有的资源。 为区块链子集提供工作的矿工得到的补偿要少于为每个可能的区块链提供工作的矿工。 小规模的矿工可能无法支付每笔区块链所需的全部费用，因此可能与较大的老牌矿工相比处于劣势，既定的可以发声的矿工可以从更多的区块链中获得更大的报酬。

然而，我们注意到矿工有可能委托验证和交易选择他们提供工作的区块链的任何子集。 选择授权可以使矿工避免几乎所有额外的资源需求，或者仍然在验证过程中为区块链提供工作。然而，这样的授权是以区块链验证和交易选择为中心的，即使工作生成本身仍然是分布式的。 矿工仍然在验证过程中也可能选择不提供区块链的工作，因此自愿放弃一些补偿，以换取更多的去中心化验证。

## 4.4软分叉的风险

在比特币中，软分叉是通过被设计成严格减少有效交易或数据块向下兼容的比特币协议的补充。一个软分叉可以用参与的绝大部分的挖掘计算能力来实现，而不是所有的完整节点。然而，参与者对软分支功能的安全性只有在升级之前仅仅是SPV级的。 软分叉已被多次用于在比特币中部署新功能和安全问题（参见[And12b]）。

按照本文所述执行的双向楔入只具有SPV安全性，因此对比比特币，它有更大的对矿工诚实度的短期依赖性（参见4.2节中描述的攻击）。 然而，如果两个系统上的所有完整节点都检查彼此的链，并要求相互有效性作为软分支规则，那么可以将双向楔入的安全性提高到绝对相当于比特币的安全性。

这样做的一个负面后果就是丧失了任何软分叉所需的侧链的隔离。 由于隔离是使用楔入侧链的目标之一，除非侧链几乎被普遍使用，否则这个结果是不可取的。然而，如果没有楔入侧链，下一个选择将是直接在比特币上部署个人变化，作为软硬件。 这甚至更加突兀，冒着比特币的风险达成共识之前，没有提供真正的机制来证明它的成熟和需求。

# 五.应用

借助技术基础，在本节中，我们将探索侧链的面向用户的应用程序，它可以有效地扩展比特币来做今天不能做的事情。

## 5.1竞争币实验

已经多次提到的第一个应用是简单地用硬币创建竞争币区块链，从而导致比特币的稀缺和供应。通过使用带有比特币而不是全新货币的侧链，人们可以避免初始分配和市场脆弱性这些棘手的问题，以及为不再需要寻找可靠市场或投资开采硬件获取竞争币资产的新用户采用的障碍。

#### 5.1.1技术实验

由于侧链在技术上仍然是完全独立的链条，所以它们能够改变比特币的特征，例如区块结构或交易链。 这些功能的一些例子是：

* 通过固定不良交易可塑性[[12]](#footnote-12)——在比特币中仅仅只有部分可被固定 [Wui14] - 可以安全地执行涉及非确认交易链的协议。 交易延展性是比特币中的一个问题，它允许任意用户调整交易数据的方式，即使事务的实际内容没有变化，以后任何依赖于他们的交易也会被中断。 一个由交易可塑性破坏的协议的例子是概率支付[Cal12]。
* 改善的付款人隐私，例如 莫内罗使用的环形签名方案可以降低被审查的特定各方交易的系统性风险，保护加密货币的可替代性。 Maxwell和Poelstra [MP14，Poe14b]和Back [Bac13a]已经提出了这方面的改进，将允许更大的隐私性。 今天，400个环形签名可以用于莫内罗币，但不是比特币; 侧链会避免这种排他性。
* 脚本扩展已经为比特币提供（例如，为了有效地支持彩色硬币[jl213]）。 由于这种扩展只能由一小部分用户使用，但所有用户都需要处理复杂性和微妙交互的风险，这些扩展并没有被比特币所接受。

其他建议的脚本扩展包括对新加密基元的支持。 例如，Lamport签名[Lam79]尽管很大，但对抗量子计算机是安全的。

* 在[Max14]和http://www.bitcoin.ninja上介绍了以不兼容的方式扩展比特币的许多想法。

由于像这样的变化只影响硬币的转移，而不是它们的创造，所以它们不需要另一种货币。用户可以用侧链安全地暂时实验。 这鼓励采用侧链，参与者使用完全独立的竞争币风险较小。

#### 5.1.2经济实验

比特币的奖励机制为矿工分配新的硬币。 这有效地影响了货币，但是随着符合计步时间表的时间的推移，它热度降低。 通过这种方式来补贴采矿是交易费用的成功补充，以保证网络的安全。

在侧链上实现块奖励的另一种机制是滞期费，这是Freicoin（http://freico.in）为数字货币开创的一个想法。 在一个有异议的加密货币中，所有未使用的产出都会超时失去价值，失去的价值被矿工们重新收回。 这样可以保持货币供应稳定，同时还能奖励矿工。与通货膨胀相比，它可能更好地与用户利益保持一致，因为滞期费的损失是无处不在的，而且是瞬间的。 同时也减轻了长期不用的“丢失”的硬币在目前的价值下被复活的可能性，并使经济震动，这是比特币中的一个可感知的风险。 滞期造成了增加货币流通速度和降低利率的激励措施，这些措施被认为是（例如Freiliin倡导者和Silvio Gesell利益理论的其他支持者[Ges16]）被认为是社会福利。 在楔入侧链中，滞期费允许矿工以现有的已估值货币进行支付。

其他经济变化包括所需的矿工费用，交易可逆性，一旦达到某个时间点时被简单删除的产出，或与侧链之外的事件楔入的浮动/滞期费率。 所有这些变化都很难安全地进行，但创造的方便性和降低侧链风险为他们提供了可行的必要环境。

## 5.2资产发行

到目前为止，我们主要考虑的是不需要自己本国货币的侧链：侧链上的所有硬币最初都是锁定的，直到它们被其他一些侧链转移激活。 然而，侧链可能会产生自己的令牌或者拥有自己的语义的资产。这些可以被转移到其他资产和货币的其他链，交换所有其他资产和货币，所有这一切都不需要信任中央党派，即使一个值得信赖的党派需要以后的赎回。

已发行的资产链有许多应用，包括传统的金融工具，如股票，债券，优惠券和借条。 这允许外部协议将所有权和转移跟踪委托给发行所有权股份的侧链。 已发行的资产链也可能支持更多创新工具，如智能财产。

这些技术也可以用于互补货币[Lie01]。 互补货币的例子包括社区货币，其目的是优先促进当地企业; 商业易货协会，这些协会支持教育或养老等社会方案; 以及在大型多人游戏，忠诚度计划和在线社区[[13]](#footnote-13)等组织内部使用的有限用途令牌。

适当扩展的脚本系统和资产认知事务交易格式将允许从审计良好的组件创建有用的事务，能为资产交换以及无信任期权(FT13)这样的复杂合同创建完全无信任的点对点市场。 例如，这些合同可以帮助减少比特币本身的波动性。

# 六.未来方向

## 6.1哈希算力攻击抗性

本文的主旨围绕使用SPV证明的双向楔入，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以便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权衡——比如，假设33%的哈希算力能使区块出一个证明，那么，要想成功使用一个假证明则需有67%的算力，依次类推。)

在侧链中其他一些值得探索的主意：

* 保证合同。除非他们的哈希算力至少，比如说，是比特币的66％，那么侧链的交易费用被矿工会给矿工。 对于加密货币来说是很容易实现的，如果从一开始就把合同设计成这样，用于提高区块转移的成本。
* 时间转换费。矿工收到的费用有些将在未来的某个区块中收到（或者分散到很多区块）以便他们可以保证维持链的工作。

这或许可以激励矿工，使其简单的收到“带外”的交易费，从而避免需要等待将来才给的链内的奖励。该方案的变式是让矿工收到一个允许挖低难度区块的令牌，将来可以使用。这是有着相同效果的，但是去挖这条链更加直接能够激励接受者。

* 滞期费。区块补贴可以用滞期费来给与矿工来激励进行诚实挖矿。由于可被转入到比特币系统或者其他侧链的数量只能和转出的一致，这种基金的重新分配兼备限定在它所发生的侧链之中。
* 补贴。一个侧链可以发行自己独立的原生货币作为奖励，这有效地形成了一个竞争币。然而，这些硬币只会有一个浮动的价值，并且结果是无法解决和竞争币有关的的波动性和市场碎片的问题。
* 合签SPV证明。引入一个必须在合法SPV证明中签字的签名者，寻找监视错误的证明。这导致了要在中心化和对抗高算力攻击之间进行直接的权衡。在这个方面有着相当大的权衡余地：签名者仅在高价值的转换中被需要，仅当侧链哈希算力过小，相当于比特币的百分之一时才会需要他们，等等。在附录A中包含对此类权衡的实用性的进一步讨论。
* SNARKs。在密码学术上最近有一个令人兴奋的进展是SNARKs的发明[BSCG+13]。SNARKs的空间效率很高，可以快速验证一些计算工作已经完成的零知识密码的证明。然而，他们的应用目前是受到限制的因为对于大多数的程序在计算机上进行验证太慢了，并且现今存在的构建需哟啊一个可信的设置，意味着系统的创建者有能力去制造假证明。

一个未来的关于低价值或者试验阶段的侧链想法是调用一个可信的机构，它的唯一任务是为SNARK方案执行一个可信任的设置。然后可以构造证明它们未花费输出出集合变更的区块，但是这是在零知识实现交易的前提下进行的。这些区块还能对于先前的区块的全部验证保证，允许只验证最新的一个区块，使新的使用者速度提升。通过一些定义的规则证明发送链的合法性，这些证明还可以取代将硬币从一条链移动到另一条链的DMMSes。

# 七.致谢

我们想要感谢Gavin Andresen,Corinne Dashjr,Mathias Dybvik,Daniel Folkinshteyn,Ian Grigg, Shaul Kﬁr, midnightmagic, Patrick Strateman, Kat Walsh, and Glenn Willen的审稿意见。

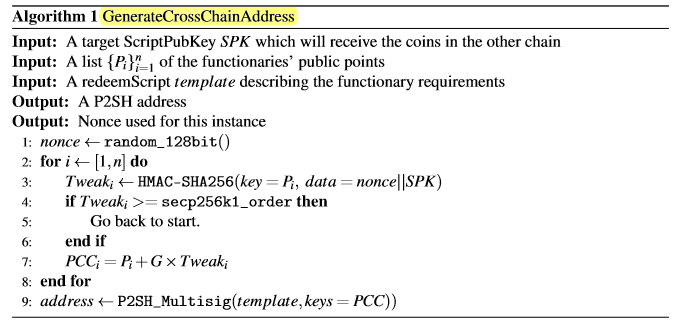
# 附录A 联合楔入

部署楔入式侧链的一个挑战是目前比特币的脚本在编码SPV证明的验证规则上，还不能够完全表达，需要一种安全、兼容并且高度分明的方式加入所需的表达（例如，通过软分叉，将一个“无操作”指令转化为一个OP-SIDECHAINPROOFVERIFY指令）。然而，建造共识并且部署这样的简单的新的功能的难度并不小。回忆这些困难正是楔入式侧链产生的部分原因。我们所想要的是有一种方法不需要各处部署就可以为比特币系统尝试未来的脚本功能。

幸运的是，通过采纳一些用低信任设计目标换取得附加的安全性假设，可以在完全无许可的情况下进行初级部署。关键的考察点是任何对比特币系统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[[14]](#footnote-14)来评估脚本，通过签发一个普通的多重签名脚本来接受。那也就是说，这些工作人员充当了协议适配器评估那些我们想要比特币去评估的但是因为缺乏脚本支持而做不了的相同规则。使用这个方法我们可以实现一种联合的楔入。

这种方法与一种建造一种多重签名链下交易的系统很相似，不过，所需的服务器到服务器的共识处理，借由简单的观察有问题的区块链来实现。结果是有了一个确定性的、高审计性的进程，简化了工作人员的选择和监督。由于这些相似性，很多用于在提高链下支付的安全性和可信度的技术，可以在联合楔入中部署。例如：工作人员在地理位置上是分散的，通过托管币，或者是托管成本高的抗胁迫的假名身份来进行担保，自爱存在远程证明的防篡改硬件上来实现，诸如此类【Tod 13】。对于一些小规模的应用，系统中硬币的持有者就可以充当为工作人员，因此避免了第三方信任。

一旦有侧链带有联合楔入被投入使用，比特币脚本中附带的SPV验证，可以被视为仅仅是一个升级来减少系统中所需信任的安全性升级。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，或是根据显见的哈希速率来切换。

考虑一个侧链使用一个工作人员联合体中5取3实现与比特币双向楔入的例子。联合体中有secp256k1公共点（共钥）P1、P2、P3、P4、P5一集一个赎回模板3 x x x x x 5 OP\_CHECKMULTISIG，所有侧链的参与者可知。要将硬币发送到脚本共钥SPK，想要硬币在一个使用联合楔入侧链可用的用户，可以按照下面的密钥方案，计算出跨链P2SH【And12a】地址：

这个推导方案是居于BIP32中使用的同等状态技术【Max11】，允许第三方导出公开的不可链接的地址。这与一个支付到交易合同的基础构建相同。产生地址后，可以将硬币支付到上面，通过将临时数，脚本共钥和SPV证明提供给工作人员来帮助他们在区块链上找到这一支付，用户随后可以收到在侧链上支付的硬币。为了帮助侧链上的第三方验证，这些价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。

联合楔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：如果联合楔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，使社区从楔入式侧链中获得信心。

# 附录B高效SPV证明

为了将硬币从一个侧链转移回到比特币系统，我们需要嵌入侧链的硬币被锁定在比特币区块链的证明，这些证明应该包含一个输出已经在侧链中被创建的记录，以及一个证明足够的工作量已经加于该输出之上的DMMS。因为比特币系统的的区块链是共享的，并被所有的参与者共同验证。这些证明必须不能给网络带来强大的负担。输出可以很容易地被紧凑记录，但是对于DMMS来说并不是那么明显能够做到的事。

紧凑型SPV安全。SPV证明的可信度可以通过将一个攻击者和诚实网络模拟为随机的处理过程【MLJ14】来证明。这些随机的过程有一个实用的统计特征：由于每个哈希值必须少于目标价值才能合法，一半时间将会得到少于一半的目标值，三分之一的时间将得到小于目标值三分之一的值，四分之一的时间将会得到少于四分之一的值，以此类推。当哈希值本身不再改变改变一个区块的计算的数目时，低于必要量的哈希值的出现实际上是在链上做了过多工作的一种统计证据。我们可以利用这一事实证明仅用几个区块头就可以达到等同的工作量[Fri14]。因而，极大地压缩区块头列表并提供仍能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。

然而，制造一个欺骗性紧凑的SPV证明和一个非紧凑型SPV证明在预期上需要的工作量是相同的，伪造成功的概率不再随被证明的工作量而指数型衰减：一个机会性较弱的攻击者有着更高的偶然成功概率。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为：

作为对比同样的攻击者在同时可以在一个区块中产生价值相当于证明1000个区块的工作量的可能性大概10％，一个相当高的数字。

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显著。

　　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)[Pug90]，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，是无法进行再平衡的)。

　　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一个前代。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，我们就可得到一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创世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

在跳过链上剩余区块前需要回向扫描的区块数估计为

因此，如果我们想用一次跳跃来跳过整个剩余链，我们预期只需检索半程即可;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。

对于一个100万区块的链，对整条链预期的证明大小仅为log2 1000000 ≈ 20个区块眉。这使DMMS的大小下降为10千字节左右的范围。

然而，正如上面所观察到的情况，如果攻击者能在仅实际开采了对外展示的区块眉时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重的链接即可。

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(cut-and-choose)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)来移动，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末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。

这使父链上的总开销与侧链的数量及长度成正比;没有这一输出，总开销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围，也超出了当前进行中的工作的主题。

# 附录C 元互换(原子交换)

一旦某侧链可运转，就有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)和长等待期。相比之下，元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(pay-to-address)的交易差不多。

有一个归功于Tier Nolanr[Nol13]的方案，工作原理如下。

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pkA和pkB，A有一个秘密数a。那么，A可以用下面的方法将币与B进行兑换：

1. 在其中一条链上，A创建一笔交易，将币移动到一个输出O1，该输出的赎回条件限制为：(a)出示a以及B的签名，或(b)A和B双方的签名。A先不广播该交易。

A创建第二笔交易，将币从O1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就可以安全地广播移动币至O1的那笔交易，A执行此操作。

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先不广播该交易。

B创建第二笔交易，将币从O2返还给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可以安全地广播移动币到O2的那笔交易，B执行此操作。

1. 由于A知道a，A能够花费O2中的币，A执行此操作，取得B的币的所有权。

当A执行此操作后，a被暴露出来，B就可以花费O1中的币，B执行此操作，取得A的币的所有权。

参考文献

[AJK05] J. Aspnes, C. Jackson, and A. Krishnamurthy, Exposing computationally-challenged Byzantine impostors, Tech. Report YALEU/DCS/TR-1332, Yale University, 2005, http://www.cs.yale.edu/homes/aspnes/papers/tr1332.pdf.

[And12a] G. Andresen, BIP16: Pay to script hash, Bitcoin Improvement Proposal, 2012, https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.

[And12b] , BIP34: Block v2, height in coinbase, Bitcoin Improvement Proposal, 2012, https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki.

[Bac02] A. Back, Hashcash — a denial of service counter-measure, 2002, http:// hashcash.org/papers/hashcash.pdf.

[Bac13a] , bitcoins with homomorphic value (validatable but encrypted), 2013, BitcoinTalk post, https://bitcointalk.org/index.php?topic=305791.0.

[Bac13b] , Re: [Bitcoin-development] is there a way to do bitcoin-staging?, 2013, Mailing list post, http://sourceforge.net/p/bitcoin/mailman/message/ 31519067/.

[Bah13] L.Bahack, Theoretical Bitcoin attacks with less than half of the computational power (draft), arXiv preprint arXiv:1312.7013 (2013).

[BSCG+13] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, SNARKs for C: Verifying program executions succinctly and in zero knowledge, Cryptology ePrint Archive, Report 2013/507, 2013, http://eprint.iacr.org/2013/507.

[Cal12] M. Caldwell, Sustainable nanopayment idea: Probabilistic payments, 2012, BitcoinTalk post, https://bitcointalk.org/index.php?topic=62558.0.

[Cha83] D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology Proceedings of Crypto82(1983), no. 3, 199–203.

[Fri14] M. Friedenbach, [Bitcoin-development] compact SPV proofs via block header commitments, 2014, Mailing list post, http://sourceforge.net/p/bitcoin/ mailman/message/32111357/.

[FT13] M. Friedenbach and J. Timón, Freimarkets: extending bitcoin protocol with user-speciﬁed bearer instruments, peer-to-peer exchange, off-chain accounting, auctions, derivatives and transitive transactions, 2013, http://freico.in/docs/ freimarkets-v0.0.1.pdf.

[Ges16] Silvio Gesell, The natural economic order, Peter Owen Ltd. 1958., London, 1916, https://archive.org/details/TheNaturalEconomicOrder.

[GH12] I. Gerhardt and T. Hanke, Homomorphic payment addresses and the pay-to-contract protocol, CoRRabs/1212.3257(2012).

[Gri99] Ian Grigg, Email correspondence, 1999, http://cryptome.org/jya/digicrash. htm.

[jl213] jl2012, OP\_CHECKCOLORVERIFY: soft-fork for native color coin support, 2013, BitcoinTalk post, https://bitcointalk.org/index.php?topic=253385.0.

[Lam79] L. Lamport, Constructing digital signatures from a one-way function, Tech. Report SRI-CSL-98, SRI International Computer Science Laboratory, October 1979.

[Lie01] B. Lietear, The future of money, Random House, London, January 2001.

[Max11] G.Maxwell,Deterministicwallets,2011,BitcoinTalkpost,https://bitcointalk. org/index.php?topic=19137.0.

[Max14] , User:gmaxwell/alt ideas, https://en.bitcoin.it/wiki/User: Gmaxwell/alt\_ideas. Retrieved on 2014-10-09., 2014.

[Mer88] R.C.Merkle,Adigitalsignaturebasedonaconventionalencryptionfunction,Lecture Notes in Computer Science, vol. 293, 1988, p. 369.

[Mil12] A. Miller, The high-value-hash highway, 2012, BitcoinTalk post, https:// bitcointalk.org/index.php?topic=98986.0.

[MLJ14] A.MillerandJ.J.LaViolaJr,AnonymousByzantineconsensusfrommoderately-hard puzzles: A model for Bitcoin, Tech. Report CS-TR-14-01, UCF, April 2014.

[Mou13] Y.M.Mouton,IncreasinganonymityinBitcoin...(possiblealternativetoZerocoin?), 2013, BitcoinTalk post, https://bitcointalk.org/index.php?topic=290971.

[MP14] G. Maxwell and A. Poelstra, Output distribution obfuscation, https://download.wpsoftware.net/bitcoin/ wizardry/brs-arbitrary-output-sizes.txt, 2014.

[Nak09] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, https://www. bitcoin.org/bitcoin.pdf.

[Nol13] T.Nolan,Re: Altchainsandatomictransfers,https://bitcointalk.org/index. php?topic=193281.msg2224949#msg2224949, 2013.

[Poe14a] A. Poelstra, ASICs and decentralization FAQ, 2014, https://download. wpsoftware.net/bitcoin/asic-faq.pdf.

[Poe14b] , Is there any \_true\_ anonymous cryptocurrencies?, Bitcoin.SE, 2014, http: //bitcoin.stackexchange.com/a/29473.

[Poe14c] , A treatise on altcoins, 2014, Unﬁnished, https://download. wpsoftware.net/bitcoin/alts.pdf.

[Pug90] W. Pugh, Skip lists: A probabilistic alternative to balanced trees, Communications of the ACM 33 (1990), no. 6, 668, ftp://ftp.cs.umd.edu/pub/skipLists/ skiplists.pdf.

[Sza97] N.Szabo,Theideaofsmartcontracts,1997,http://szabo.best.vwh.net/idea. html.

[Tod13] P. Todd, Fidelity-bonded banks: decentralized, auditable, private, off-chain payments, 2013, BitcoinTalk post, https://bitcointalk.org/index.php? topic=146307.0.

[vS13] N. van Saberhagen, Cryptonote v 2.0, https://cryptonote.org/whitepaper. pdf, 2013.

[Wui14] P. Wuille, BIP62: Dealing with malleability, Bitcoin Improvement Proposal, 2014, https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki.

1. \*adam@cypherspace.org, mattc@bluematt.me, luke@dashjr.org, mark@friedenbach.org, greg@xiph.org, amiller@cs.umd.edu, apoelstra@wpsoftware.net, jtimon@jtimon.cc, [pieter.wuille@gmail.com](mailto:pieter.wuille@gmail.com)

   †这工作得到了几位作者创立的Blokstream公司的部分支持。本文讨论的许多概念都是在Blockstream存在之前讨论的，侧链技术是一个作者自己提出的开放建议。 [↑](#footnote-ref-1)
2. 承诺是一个密码对象，它是从一些秘密的数据计算出来的，但是并没有揭示它，使得数据在事后不能被改变。 承诺的一个例子是散列：给定数据x，可以发布H（x），其中H是散列函数，并且只在稍后显示x。 然后验证者可以通过计算H（x）本身来确认显示值与原始值相同。 [↑](#footnote-ref-2)
3. 我们以比特币为例，因为它强大的网络效应使用户可能更喜欢其他新的资产。 但是，任何一款竞争币都可以改编成可用于侧链。 [↑](#footnote-ref-3)
4. 在客户当地发生的重组或重组，使得通过更多的工作证明通过链接进行交易，从而导致叉的任何阻碍被从共识历史中移除。 [↑](#footnote-ref-4)
5. 这也被称为单向楔入，与之后介绍的双向楔入形成鲜明对比。 [↑](#footnote-ref-5)
6. 当然，侧链能够支持他们自己的资产，他们将负责保持稀缺性。 我们的意思是强调他们只能影响自己和子链的匮乏。 [↑](#footnote-ref-6)
7. 几乎在比特币的所有方面都是如此：运行完整节点的用户决不会接受直接或间接由于伪造或没有证明拥有的交易花费。 然而，不可靠的操作是不可能的，因为没有办法区分两个冲突但是有效的交易。 比特币不是像依靠比特币的前任那样依靠集中信任的一方或多方来承担这种仲裁功能，而是通过使用DMMS和经济激励措施来降低所需的信任，但不会消除信任。 [↑](#footnote-ref-7)
8. 以【Nak09】中的“简化交易证明”在本节后 [↑](#footnote-ref-8)
9. 在比特币中，只需要使用一组未使用的交易输出（UTXO's）来确定所有硬币的状态。 通过构建Merkle树[Mer88]，我们可以仅使用一个散列来承诺UTXO集的每个元素，从而最小化区块头空间的使用。 [↑](#footnote-ref-9)
10. 软分叉变化是对链条内部有效性进一步限制的变化。 有关更多信息，请参阅第4.4节。 [↑](#footnote-ref-10)
11. 这意味着使用DMMS不仅可以确定交易顺序，而且可以确定其有效性。 换句话说，这意味着相信矿工不会产出无效块。 [↑](#footnote-ref-11)
12. 请注意，某些形式的延展性是需要的（即由SIGHASH\_flag提供的SIGHASH\_ALL以外的类型）。 [↑](#footnote-ref-12)
13. 有关补充货币的更多信息，请参阅http://www.complementarycurrency.org/ [↑](#footnote-ref-13)
14. 从维基词典（https://zh.wiktionary.org/wiki/functionary）来说，一个工作人员是一个人......他拥有有限的权力，主要是为了执行一个简单的功能而不需要任何裁量权。我们用这个词来强调，虽然工作人员具有破坏侧链之间转移的实力，但他们的正确操作是纯粹的机械的。 [↑](#footnote-ref-14)