侧链白皮书：用楔入式侧链实现区块链的创新—摘要、前言

**[chehw](http://www.8btc.com/author/326" \o "由 chehw 发布) 2014-10-28 10:55 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**30**](http://www.8btc.com/enabling-blockchain-innovations-with-pegged-sidechains-abstract-introduction#comment)**12741**

**摘要**

自2009年比特币系统的推出以来，它带来了众多计算机科学和电子现金方面的创新，人们对去中心化加密货币的潜力有了极大的兴趣。但与此同时，对已达成共识的比特币系统关键部分实施变更，则必须非常保守地来处理。这导致与其他互联网协议相比，比特币系统更难于适应新需求和采纳新创新。

我们提出了一种新技术——“楔入式侧链”——实现比特币和其他帐簿资产在多个区块链间的转移。这使用户能用他们已有的资产来使用新的和创新的加密货币系统。通过复用比特币系统的货币，这些系统相互之间的交互操作，以及与比特币之间的交互操作，可以更容易地进行，避免出现与新货币相关的流动性短缺和市场波动。由于侧链是独立的系统，技术和经济上的创新不会被其他因素妨碍。尽管比特币系统和楔入式侧链间有双向转移的能力，但它们是隔离的：即使出现侧链中加密被破解（或恶意设计）的情况，所有的损害都只限于侧链本身。

本文将阐述“楔入式侧链”及其实施要求，以及为了能从将来区块链间的互联中充分受益所需的工作。

－－－－

[](http://7fvhfe.com1.z0.glb.clouddn.com/%2540%252F%2F/wp-content/uploads/2014/10/sidechain1.png)

**目录**

1 前言

2 设计原理

3 双向楔入  
3.1 定义  
3.2 对称式双向楔入  
3.3 非对称式双向楔入

4 缺陷  
4.1 复杂度  
4.2 欺骗性转帐  
4.3 中心化挖矿的风险  
4.4 软分叉的风险

5 应用  
5.1 竞争链实验  
5.1.1 技术实验  
5.1.2 经济实验  
5.2 资产发行

6 发展方向  
6.1 抗哈希算力攻击

7 致谢

A 联合楔入  
B 高效SPV证明  
C 元互换

**1 前言**

1983年，David Chaum将数字现金作为一个研究课题首次提出，通过设置一个可信的中央服务器，来防止双重花费[Cha83]。为降低这个中央可信方带给个人的隐私风险，并确保资产的可置换性，Chaum引入了盲签名——提供一种加密方法，来防止与中央服务器的签名（这个签名代表钱币）进行关联，同时还能让中央服务器进行双花防范。对中央服务器的需求，是数字现金的致命弱点（阿喀琉斯之踵）[Gri99]。虽然有可能通过将中央服务器的签名替换为含几个签名者的门限签名，来分散单点故障，但区分和辨识签名者的可审计性变得很重要。在这种方法下，系统仍然易出故障，因为每个签名者都可能会出问题，或者是一个接一个地被人为制造出问题。

2009年1月，中本聪发布了第一个广泛使用的点对点无信任电子现金系统，用基于工作量证明的共识机制来替代中央服务器的签名，用经济上的激励实现协同工作。比特币通过聚合成区块的方法来跟踪支付，每个区块关联有一个区块眉（blockheader），用密码学方法来指代（承诺）：区块的内容、时间戳、前一个区块眉。到前一区块眉的“指代”（commitment）构成了区块链，或者说是提供了一个明确交易次序的链。（译者注：在密码学中，commitment指的对原始数据用加密算法进行处理，生成的摘要可以在不泄露原文的情况下可以有效地代指原始数据。有些文章将commitment译为“承诺”或“秘诺”，本文中译为了“指代”）

我们注意到，比特币系统的区块眉可以看作是动态成员多方签名(或称DMMS)的一个实例，我们认为它作为群签名的一种新类型，有独立的价值。尽管截止目前的文献中尚未提及，比特币系统提供了这种签名的第一个实施方案。一个“动态成员多方签名”（DMMS）是由一组数量不固定的签名者所形成的数字签名。比特币系统的区块眉是DMMS，因为其工作量证明机制具有让任何人无需登记即可献力的特征。此外，贡献量不是让每个参与方提供一个门限签名，而是通过计算力来衡量，这可以允放使用匿名成员身份，并且不会有女巫攻击(Sybil attack)的风险（一个参与方多次加入，获取在签名中不相称的输入份额）。基于这个原因，DMMS也被描述为是拜占庭将军问题的一个解决方案。

由于区块是链接在一起的，比特币系统的DMMS是累积的：任何一个区块眉的链（或链的片断）都是第一个块的DMMS，其计算强度等于组成它的全部DMMS之和。中本的关键革新就是如上所述的，使用了基于计算力的DMMS签名，而不是基于知识的签名。由于签名者是证明其计算工作，而不是典型数字签名中的证明其私密知识，我们称这样的签名者为“矿工”。为了获取区块链历史的稳定共识，系统提供了经济激励，只有当矿工们构建了可共享的有效历史记录，他们获取的钱币形式的交易费和奖励才会有价值，这激励他们诚实地工作。因为比特币的累积DMMS强度与所有矿工们贡献的计算力成正比，算力占少数的一方想改变链是行不通的。如果他们试图修改受DMMS保护的帐簿，他们就会落后，并且一直无法追上达成共识的区块链的进度。

由于矿工们并没有形成一个可辨识的集体，他们对决定交易有效性的规则没有自由裁量权。因此，比特币的规则必须在它的历史初期就要确定，除非每个网络参与者达成一致，否则新的有效交易类型无法添加进来。即使能达成这样的一致，变更的部署实施也很困难，因为这需要所有参与者都要用相同方式落实和执行新的规则，还要考虑到边缘情况以及其他因素导致的意外的影响。

正因如此，比特币系统的目标相对简单：它是一个支持单一原生数字资产传输的区块链，不能与其他任何资产相兑换。

这可以简化很多具体实现，不过这样的简化正面临着现实世界需求的挑战。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，代价是加大了验证方的工作量——中心化的风险。

同样，在安全性和成本之间也存在取舍。比特币历史记录中用同等级别的不可逆性存储了每一笔交易。这种方式的维护代价很高，对低价值和低风险的交易来说也未必合适（例如，所有参与方已经商定了一个共同的法律机构来处理欺诈行为）。

由于不同交易的价值和风险状况有很大的不同，这样的取舍应当针对每笔交易来应用。然而比特币系统的构建仅支持以一个标准来应对所有问题。

2．在区块链的功能上存在更多的取舍。例如，是让比特币的脚本更强大来支持简明和有用的合约，还是减少功能以便于审计。

3．一些非货币的资产也可以在区块链上交易，例如欠条、其它合约和智能财产。

4. 存在一元化育成的风险:比特币系统由许多密码学组件构成，其中的任何一个组件出问题，都会导致整体价值的损失。如果有可能，不要用同一套算法来保护每个比特币会更谨慎些。

5．新技术可能会带来比特币系统创建初期没有想到的新功能。例如，用加密累加器、环签名或Chaumian盲签名来增强隐私保护和抗审查性。

6．即使有这样做的迫切需求，但没有对比特币系统安全升级的途径，这意味着任何更改都需要所有参与者协同执行才能生效。比特币的开发者们之间达成了一个共识，对比特币系统的变更必须缓慢、谨慎，且仅当社区有明确同意时才进行。