比特币和加密货币的研究前景和挑战

*Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A.Kroll, Edward W.Felten*

*∗Princeton University, †Stanford University, ‡Electronic Frontier Foundation, §University of Maryland, ¶Concordia University*

**摘要：**比特币已经成为历史上最成功的加密货币。尽管比特币只是对系统设计的粗略分析，但是在2009年比特币悄悄发布的两年内，比特币增长了十亿美元的经济价值。自从那时起，越来越多的文献已经鉴定了这个系统隐藏但是重要的属性，发现了攻击方式，提出了有前途的替代品，同时也发现了它未来艰巨的挑战。与此同时，一个巨大并且充满活力的开源社区提出并做出了大量的修改和扩展。

我们提供了第一个有系统性阐述的比特币以及许多相似相关的加密货币。从分散的知识体系开始，我们确定比特币设计的三个关键组成部分可以分离。这使得关于比特币的性能和未来稳定性的分析变得更有见地。我们为众多提议的修改保留了设计空间，并为替代共识机制、货币分配机制、计算难题以及关键的管理工具提供了比较性分析。我们调查了比特币中的匿名问题并提供了一个评测框架来分析各种增强隐私性的提议。最终，我们提供了一个有关我们所谓的非中介性协议的新见解，非中介性协议在一组有趣的应用程序中解除了对可信中介的需求。我们确定了三个普遍的非中介性策略并提供了详细的对比。

**SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies**

Joseph Bonneau∗†‡, Andrew Miller§, Jeremy Clark¶, Arvind Narayanan∗, Joshua A. Kroll∗, Edward W. Felten∗

∗Princeton University, †Stanford University, ‡Electronic Frontier Foundation, §University of Maryland, ¶Concordia University

Abstract—Bitcoinhasemergedasthemostsuccessfulcryptographiccurrencyinhistory.Withintwoyearsofitsquietlaunch in2009, Bitcoin grew to comprise billions of dollars of economic value despite only cursory analysis of the system’s design. Since then a growing literature has identiﬁed hidden-but-important properties of the system, discovered attacks, proposed promising alternatives, and singled out difﬁcult future challenges. Meanwhile a large and vibrant open-source community has proposed and deployed numerous modiﬁcations and extensions. We provide the ﬁrst systematic exposition Bitcoin and the many related cryptocurrencies or ‘altcoins.’ Drawing from a scattered body of knowledge, we identify three key components of Bitcoin’s design that can be decoupled. This enables a more insightful analysis of Bitcoin’s properties and future stability. We map the design space for numerous proposed modiﬁcations, providing comparative analyses for alternative consensus mechanisms, currency allocation mechanisms, computational puzzles, and key management tools. We survey anonymity issues in Bitcoin and provide an evaluation framework for analyzing a variety of privacy-enhancing proposals. Finally we provide new insights on what we term disintermediation protocols, which absolve the need for trusted intermediaries in an interesting set of applications. We identify three general disintermediation strategies and provide a detailed comparison.

# 为什么比特币值得研究

考虑两个关于比特币草案形式的对立观点。第一点是“比特币只在实践中起作用，但不是在理论上”。有时，比特币社区的成员奉行这一理念，并批评安全研究界未能发现比特币，并未立即认识到其新颖性，而且由于缺乏严密的理论基础，至今仍然对其不屑一顾。

第二个观点是比特币的稳定性依赖于一个未知的社会经济组合，这个因素难以精确地模型化，没有为系统的健全性产生让人信服的论据。鉴于这些困难，经验丰富的安全研究人员可能会避免将比特币作为研究的主题，考虑到审慎的安全工程只能设计具有精确的威胁模型的系统，以承认其形式化的安全证明。

我们打算展示每个这些简单化的观点失败的地方。首先，我们认为尽管到目前为止比特币在实践中已经出乎意料地发挥了强大作用，但是研究室在判定为什么比特币发挥巨大作用是可能的中扮演了重要的角色，超越了对与系统最初提案一同提出的非正式论点的盲目接受。此外，了解比特币是否会随着实践的变化而在实践中工作是至关重要的。我们期望随着外部政治和经济因素发生变化，如果交易量增加，系统必须改变，作为系统设计的一部分，比特币矿工的货币回报的性质将随着时间的推移而变化。这并不足以表明比特币已经从2009年工作到2014年并将继续下去的事实。我们还没有足够的理由来断定比特币在实践中会继续良好运作，这是一个至关重要的研究挑战，需要计算机科学理论的支持。

对于第二个观点，我们认为比特币是通过提供没有任何可信任的参与者虚拟货币系统并且在参与者之间没有预先假定身份的情况下填补了一个重要的利基。在这些约束条件下，如果没有像比特币这样的前提假设，可以模拟理性(贪婪)行为，可以调整激励机制，以确保协商一致算法的安全运行，分布式系统中普遍存在的共识系统是不可能的[7],[93]。然而，无论在哲学上还是在技术上，这些约束在实践中很重要，比特币在这个模型中达成共识的方式是令人惊讶的根本性贡献。比特币的核心共识协议还对货币之外的许多其他计算机安全问题产生了深远的影响[[1]](#footnote-1)，例如：分布式命名、安全时间戳和承诺，公共随机生成以及许多财务问题，例如：自我实施（智能）合同、分散市场和订单簿以及分布式自治代理。简而言之，比特币虽然不容易建模，但值得大力研究，因为它可能成为实际解决极端困难和重要问题的基础。

考虑到这种二分法，我们着手综合比特币运作和发展的前六年以及其衍生的许多加密货币的集体知识。我们的目标是既突出从新型支付协议到用户友好的密匙管理出现的重大创新领域，也突出比特币和未来加密货币最重要的开放性研究挑战。

# 比特币概述

## 情境化的历史

我们将感兴趣的读者引用到现有的关于加密货币研究的“第一波”的调查中[15],[95]。简而言之，加密货币可以追溯到1983年Chaum关于“难于追查的付款”的提议[28]，这个系统包括银行发行的以盲目签署的硬币形式的现金。非盲目的硬币在用户和商家之间转移，并且在银行核实之后可以兑换。盲目签名阻止银行将用户链接到硬币，提供类似于现金的不可链接性。整个20世纪90年代，这个方案的许多变化和扩展被提出。重要的贡献包括在购买时不需要银行上网[29]，硬币被分成更小的单位[92]，并提高效率[27].包括数字现金（DigiCash）[107]和点点币(Pepeercoin)[99]在内的几家初创公司试图将电子现金协议付诸实践，但最终在市场上失败了。从这个加密货币研究的“第一波”中没有任何方案实现了重要的部署。在20世纪90年代早期，比特币的一个关键组成部分就是中等强度的“校对工作”难题，它在90年代被提议用于打击垃圾邮件，虽然从未被广泛部署过用于这个目的。许多其他应用程序，包括公平彩票的建议[51]，小额铸币[100]，并反正告知各种形式的拒绝服务和滥用匿名网络[10]。后者哈希现金(Hashcash)是使用数字微支付（如：Netbill[110]和Karma[121]）的一种替代方案。工作证明也用于检测分布式点对点共识协议中的sybil节点[7]，类似于目前在比特币共识中的使用。

比特币的另一个重要元素是公簿，这使得双重支出是可检测的。在1990年代后期提出的可审计的ecash[105]，[106]中，该银行维持一个公共数据库来检测双重支出并确保硬币的有效性，但是公布整套有效硬币的概念被认为是不切实际的（只发布了一个Merkle根）。1998年提出的B-money似乎是所有交易都是公开（匿名）广播的第一个系统。在Cyherpunks邮件列表上的提议，B-money收到了学术研究界的最少关注。

在20世纪90年代早期提出的智能合约[114]使各方能够正式指定一个可执行加密协议，预示比特币的脚本功能。

在2008年，比特币被宣布，以笔名Satoshi Nakamoto写的白皮书被张贴到Cyherpunks邮件列表[90]，紧随其后的是原始参考客户端的源代码。比特币第一个区块链是在2009年1月3日[[2]](#footnote-2)左右开采的.比特币第一次作为货币的使用是2010年5月的一笔交易，其中一个用户订购比萨饼交付对方10,000比特币。此后，越来越多的商家和服务采用比特币，价格普遍上涨，2013年末达到每比特币1200美元的高峰。

比特币的历史也因其与犯罪的关系而变得色彩斑斓。流行的黑市网站SilkRoad [30]从2011年10月开始运行，直到2013年10月被联邦调查局查封和关闭。僵尸网络已经发现比特币挖掘是个补充收入的来源[57].目前的美国联邦法院案件涉及庞大的比特币庞氏骗局[109]. 2014年，一种名为CryptoLocker的电脑病毒通过对其文件进行加密并要求比特币赎金释放解密密钥，从受害者身上勒索了数百万美元[47]。 许多用户的比特币由于被盗窃[41]和交换失败[86]而丢失。

## 技术概述

我们介绍比特币的三个主要技术组件：交易（包括脚本），共识协议和通信网络。比特币是非常复杂的——我们的目标是以充分科技深度的系统来研究比特币的文献，并且在后续论文章节中进行回顾和评估。尤其是，我们的三个组成部分的一个关键好处是它通过“独立”的概念来进行评估和系统化（第六和第八部分）。

**关于比特币的信息的来源。**比特币可能难以定义，因为没有权威的正式规范。原先的比特币白皮书[90]提供了比特币设计理念的很好的概述，但是许多重要的技术细节被忽略或过时。参考贯彻比特币客户端被认为是一种事实规范，分散在一系列“比特币改进提议”(BIPs), 论坛发布，在线wiki文章，开发者邮件列表以及登录的IRC讨论中[[3]](#footnote-3)我们将这些资源进行系统化 进行精确的技术介绍，提出我们认为是独立设计决策的系统组件。

1）交易和脚本：比特币在世界中的状况是由一系列称为交易的信息来表示的。在其他可能性中，交易最重要的是将货币从一个用户转移到另一个用户。 值得注意的是，大型（和不断增长的）交易清单是比特币中唯一的状态。比特币没有内部的概念，比如用户、账户余额或者身份这些更高层次的概念——这些董只存在于已发布的交易清单中。

**交易格式。**一个交易包含一组输入和一组输出。整个交易使用SHA-256[[4]](#footnote-4)散列，并且这个散列最终[[5]](#footnote-5)作为其全局唯一的交易ID。 交易使用特别的二进制格式表示; 这是一个重要细节的早期例子证明了比特币客户端是事实的详述。

每个输出包含一个代表比特币数量的整数值。 这个数值的精确度限制了货币单位可以细分的程度; 最小的单位叫做satoshi。 按照惯例，108 satoshis被认为是货币的主要单位，称为一个“比特币”[[6]](#footnote-6)，表示为BTC或XBT。

每个输出还有一个简短的代码片段（用一种特殊的脚本语言），称为scriptPubKey，表示代表可以兑换交易输出的条件，也就是在后面的交易中作为输入。

**交易记录。**通常情况下，脚本编辑器指定ECDSA公共密钥和签名验证例程的散列值。 这被称为“付费到发布 - 密钥 - 散列”交易，整个兑换交易必须使用具有指定散列的密钥进行签名。 绝大多数比特币交易是付费到发布 - 密钥 - 散列，并且系统通常被描述为这是唯一的可能性，尽管其他交易类型是可能的。 脚本语言是一种特殊的，非图灵完备的堆栈语言，其命令少于200个，称为操作码。 它们包括对密码操作的支持，例如哈希数据和验证签名。 就像事务处理格式一样，脚本语言只能通过比特币客户端的实施来指定。

交易输入通过交易散列和交易输出数组内输出的索引来引用前面的交易。 他们还必须包含一个代码片段，用于“赎回”称为scriptSig的事务输出。 要成功兑现前一个事务，scriptSig 和scriptPubKey必须一个接一个地使用相同的堆栈成功执行。 对于付费到发布 - 密钥 - 散列交易，scriptSig只是一个完整的公钥（带有正确的哈希）和一个签名。

**保值。**除了要求每个交易输入与之前的交易输出匹配并且两个脚本成功执行之外，交易只有在满足基本约束时才有效，即所有交易输出的值的总和小于或等于所有投入的价值。我们讨论第Ⅱ-B2部分中的一个例外：用于创建新货币单位的比特币公司交易。

**从交易到所有权。**这种交易方式本身就意味着一些有趣的特性. “拥有”比特币的身份或个人账户没有固有的概念。 所有权仅仅意味着知道一个私钥，该私钥能够兑换某些产出的签名 - 个人拥有尽可能多的兑现比特币。 公钥哈希，如付费到发布 - 密钥-哈希交易中指定的那样，在系统内有效地用作假名身份，并被称为地址。 没有真实世界的名字或识别信息是必需的。

可以说，对于比特币的交易格式来说，没有多少创新。 然而，使用脚本语言来指定兑换标准以及事务可以指定整个系统状态的实现是以前的加密货币系统的非明显的设计选择，这两者在基本上所有的后续设计中都是标准的。 一些提议扩展了比特币交易的语义（通常通过增强脚本语言），而不改变任何其他组件。

2)共识与挖掘：如果在用户之间直接发送交易以转移资金，那么以交易为基础的货币体系将是不安全的。尽管签名会限制前一个交易的有效收件人参考无效的追加交易，但交易本身并没有限制Alice在发送给Bob和Carol的单独交易中两次兑换某些交易输入，这两个交易似乎都是孤立的。比特币采用一种简单的方法来解决这种双重支出攻击：所有交易必须在全球性的永久性交易日志中发布，任何单个交易输出只能在一个后续交易中被兑换。现在验证交易需要验证交易的脚本，并确保将其成功发布到日志。在比特币中，日志是作为一系列交易块来实现的，每个交易块都包含前一个块的散列，将这个块作为唯一的前件。它被称为区块链。

请注意，这种设计仍需要区块链内容的全球共识。 如果鲍勃和卡罗看到两个不同的区块链，他们将容易受到双打的攻击。 一个解决方案是使用可信的中央权威机构收集交易并将其发布在有符号的块中。 然而，这是不可取的，因为这个机构可能拒绝发布某些交易（有效地冻结用户的资产），可能完全失败，或者可能故意将区块链分叉，以双倍花钱。

中本聪共识。比特币通过一个分散的，被称为中本聪共识的假名协议在区块链上建立了共识。这可以被认为是比特币的核心创新，也许是其成功最关键的因素。任何一方都可以尝试通过收集一组有效的未决交易添加到链中并形成一个块。核心要素是使用一个具有挑战性的计算难题（通常用一个用词不当的词来表示：proof of work[[7]](#footnote-7)（工作量证明）），以确定哪一方的区块将被视为链中的下一个区块。选择一个新块的过程很简单：包含计算问题解决方案的第一个公布的有效块被认为是正确的。 听到这个消息，其他参与者就开始寻找后续块。 如果已宣布的块包含无效交易或其他格式错误，则所有其他参与者都将拒绝并继续工作，直至找到有效块的解决方案。 在任何时候，共识区块链都是“最长”的版本。 通常情况下，这只是最多块的分支，但由于长叉的挖掘困难可能不同，所以最长的链必须被定义为最难产生的链[[8]](#footnote-8)。

在大约同一时间找到两个有效的解决方案（取决于网络延迟）也是由可能的，这会导致临时分叉，在这个分叉期间存在两个等长链。使用者可以选择这个方案。由于计算难题的随机性，一个区块链将最终延伸到另一个区块，在这一点上所有的矿工应该采用它。

虽然比特币的原始规范只提供了一个非正式的论点，最终达成了共识[90]，但后续工作证明，假设一个有效和及时的广播频道，控制大部分计算能力的矿工忠实地遵循协议，协议是强大的，网络逐渐达成共识[46],[84]。我们将在第三节进一步讨论这一点。

**区块鉴定。**这种共识机制的渐进性意味着用户必须等待块被发现，以获得高度的可信度，交易记录会永久地被包含在区块链中。在一个分叉期间，其中一个分支最终会在矿工聚集到另一个分支后被丢弃。尽管两个分支通常都包含大部分相同的交易，但如果冲突交易包含在竞争分支机构中，则显然可以包含在最长的一个链中，但如果另一个分支超过它，则被撤销。 在最坏的情况下，这可以有效地实现双重支出攻击[12]，[60]。

从理论上讲，用户永远不能完全确定一个交易最终会不会被一个非常深刻的分支去除[13],[70]。然而，如果大多数矿工遵循缺省协议，则用户可以推断交易越来越可能（参考第III-A部分）以最终最长的链条作为结果块被发现。 实际上，大多数比特币客户端在接受交易发布之前需要6个“确认”块。 6块的选择是任意的，它来源于参考客户端，并不基于对深叉概率的任何分析。

深度分叉也可以通过在默认的比特币客户端中包含硬编码的区块链前缀（检查点），以特定的方式防止客户端在任何有效的区块链中使用。 劳里[70]认为，这些检查点表明，比特币不是一个真正的分散的共识协议，因为它们是以集中方式选择的。

**激励正确的行为。**该协议的一个关键组成部分是发现一个块的参与者可以插入一个比特币交易，将指定数量的货币转移到他们选择的地址中。因为参与者为了得到金钱奖励而工作（实际上是竞赛）来解决这个计算难题，所以他们被称为矿工。这种被成为区块奖励的新比特币激励了矿工只能在有效区块上工作，因为无效的区块将被网络拒绝。，而他们的挖矿奖励将不会存在于最终最长的区块链中。请注意，从矿工的角度来看，“有效的”块只是那些他们认为大多数其他矿工会接受和建立的块，超过了任何其他有效性的规定（除了比特币实施之外没有其他规定）。

由于这种共识算法依赖于矿工的金钱回报，因此不容易在没有可转让价值概念的系统中使用。 在比特币中，矿工最初收到所有新货币，没有其他允许的货币创造机制。 这并不是绝对必要的，但是共识协议确实要求向矿工发放一些奖励，否则他们没有动力找到有效的块并解决困难的计算难题。

**挖掘细节。**计算难题本身需要为SHA-256（一种加密散列函数）发现部分预映像。 具体而言，难题是找到一个块（由交易清单，前一个块的散列值，时间戳和版本号，以及一个任意的临时值组成），其中SHA-256以散列值的形式出现。 这个难题常常被描述为发现一个以d个连续的零位开始的散列[[9]](#footnote-9)。标准策略是简单地尝试随机值[[10]](#footnote-10)直到找到一个解（尽管这可能不是唯一的策略[34]）。

这个难题的随机性是重要的；用非随机的难题（真正的工作证明），则最强大的个体矿工可能会首先找到每个块。随机难题中，每个矿工发现下一个区块的概率与其计算能力的份额成正比。

难题的难度经过校准，使得平均10分钟能找到一个新的区块。为了保证这一点，每隔2016个区块或者大约两星期会进行一次难度调整，以之前2016个区块的时间戳的确定性函数为准[[11]](#footnote-11)。

**挖掘奖励和费用。**区块奖励的大小由一个固定的时间表决定。最初，每个区块的创建奖励50个比特币，这个数字已经减半到25个比特币，并且计划大约每四年减半，直到大约2140年，在这个时候，不会再有新的比特币产生。

为了减少创造货币的风险，矿工们不仅可以从区块奖励中获益，他们也可以索要在这个区块中的所有投入和所有产出交易之间的净价值差异。因此，对于用户而言，一个输入值大于输出值的区块应当包括支付给矿工的交易费。

迄今为止，交易费主要用于阻止过多的小额交易（称为小额信贷）使用网络，交易费从未提供超过1-2%的矿业收入[87]。费用主要由参考客户端配置的默认值决定[87]，少数用户选择支付更高的费用来快速地发布其交易。

**矿池。**在实践中，矿工通常与矿池合作[102]，通过与其他一些矿工共享回报来降低他们收入的风险。矿池往往由一位经理负责管理，他只收取少量费用，从所有参与成员发现的有效区块中收集采矿奖励，并按照他们代表池所进行的工作量比例将资金分配给成员。 参与的矿工通过发送散列开始的大量“零”（概率）“近块”来证明他们已经完成的工作量（比如d`= 40），但是它们并不是有效的比特币区块。 由于风险分担，池中成员获得的回报差异较小，以换取预期收入的小幅下降来支付经理费用。

尽管原始议定书中没有描述“池”，也可能没有预料到，但自2013年以来，大部分采矿权被组织到“池”中。 一些公式被用来分配“池”成员之间的收入，以鼓励忠诚度，并尽量减少“跳池”，同时对新成员友好[102]。 从“池”操作者到成员[94]之间以及不同池的操作者之间也有几个标准的低延迟通信协议[32]，[74]。 虽然最受欢迎的池是集中管理的，但也有使用P2Pool协议的特殊池[122]。

3）点对点通信网络：比特币的最终核心部分是它的通信网络。 本质上，它是一个分散的，特设的点对点广播网络，用于宣布新的交易和提出的区块。 一般来说，这是三个组成部分中创新最少的一个，而且很少有人做出实质性的改变。

**共识的影响。**由于两大原因，网络的性能和稳定性对共识协议由重要的影响。首先，发现一个数据块与其他所有节点接收数据之间的等待时间增加了临时分叉的可能性。对频繁分叉的恐惧促使10分钟成为了原始设计中的区块创建时间。 其次，一个能够控制大部分网络的恶意挖矿者可能会试图利用他自己区块的广播，从而增加了区块“分叉”的可能性，从而增加了预期的回报。类似地，任何能够检查网络的部分都可以有选择地阻止传输和冻结资产。 因此，比特币拥有分散的广播网络（整体设计），低延迟以及难以检查或延迟信息是非常重要的。

**网络拓扑和发现。**任何节点都可以通过连接到其他节点的随机样本来加入网络。 默认情况下，每个节点尝试进行8个传出连接，并准备接收多达125个传入连接。 NAT之后的节点（如移动客户端）无法接收传入的连接。 那些加入这个网络的同行们最初想要找到其他的同伴。 像许多其他的点对点网络一样，比特币通过使用专用目录服务器或“种子节点”来实现这一点，比特币的身份被硬编码到参考客户端中; 此后，每个节点维护它所知道的列表中的对等节点地址。

对等节点还通过其他两种机制传播彼此的信息：首先，当一个节点建立一个新的传出连接时，它会触发一系列包含连接信息的中继消息; 其次，在收到一个传入的连接后，一个节点询问来自其已知地址列表的一个样本。 这种机制建立了一个连接良好的随机网络，具有低等级但低直径的特点，适合通过扩散快速播送信息[38]，[61]。

**通信协议。**新区块和待处理交易通过冲刷的方式播送到整个网络。一旦节点发现包含新区块或未决交易的节点，节点会发送INV消息给他们。如果这些节点没有发现信息，节点能够通过请求这些块或者交易的全部内容来做出响应。默认情况下，节点只会转发一次新的数据，防止无限的广播；只会传递交易或者有效区块；只会传递两个区块短暂分叉时听到的第一个区块，不会传递与他们发送的待处理信息冲突（双重支出）的未决交易。这些限制能优化性能，旨在限制网络上的数据-非兼容节点可能中继无效数据或冲突数据，要求所有节点独立验证接收到的所有数据。这些限制是优化性能的，旨在限制网络数据——非兼容节点可能传递无效或冲突数据，这要求所有节点独立验证接收到的所有数据。

**传递政策。**在默认情况下，比特币节点只传递比通用交易有效性规则更严格验证规则的交易与区块。我们的目标是防止各种阻断服务攻击——一个典型的稳健性原则的应用“发送时要保守，接收时要开放”。例如：默认节点只传播包含来自非常狭隘的白名单的标准交易类型的交易。这个政策的含义是，希望在区块链中包含非标准交易的系统的用户不能使用正常的比特币网络，而是需要直接联系一个合适的矿工[[12]](#footnote-12)。另一个例子是，默认节点拒绝以低于每分钟0.001比特币的报酬传输几千个事务。

# 比特币的稳定性

通过许多模糊的，甚至有时是相互冲突的方式，比特币的稳定性已经被评定，但是广义上的意思是，随着其增长和参与者尝试新型攻击，系统将继续以促进功能性货币的方式行事。在比特币稳定的确切条件下，这仍然是一个悬而未决的问题，虽然稳定性结果存在于强烈的假设下。

## A.交易有效性规则的稳定性

比特币生态系统的参与者如何就交易有效性规则达成共识，这一点是欠缺的。基本的理念是，这些规则由中本聪设定的，我们称之为规范主义。这已经介绍了一些关于指定规则的分歧，比如原始OP\_CHECKMULTISIG操作码中的一个良性漏洞已经被保留为规范。

然而，规范主义并不能完全解释当前的比特币规则，因为已经实施了增加新功能的变化（例如付费—脚本—哈希[2]）。 规则也被修改来修补漏洞，最著名的例子是2013年3月发生的，当时限制了有效块大小的bug被移除了。 这导致了一个新的分叉，更大的块被未打补丁的客户拒绝。 为了解决这个问题，更新的客户端放弃了一个24块的分支，并暂时停止在较长的客户端升级期间的两个月窗口中包含更大的块[1]。 然而，最终，这个错误已经得到解决，尽管可以说实施了规范的规则，但是未打补丁的客户最终被排除在外。

就比特币本身，没有一个进程被指定用于更新交易有效性规则。没有矿工的一致支持，任何改变都有可能永久性地影响整个系统，不同的人群考虑到最长的区块链反映他们对规则的解释是真实的，而不管其相对于其他区块链的长度如何。 在这一点上，将不再清楚哪个版本是“比特币”。因此，尽管比特币是一个完全分散的系统，但是对规则变化（或消歧）的需求意味着为了维持关于哪个区块链被视为比特币的真实世界共识，需要一定程度的治理 [48]，[64]。

目前，实际的治理由比特币基金会的核心比特币开发者提供，比特币基金会提供了一个基本的组织结构，并通过捐助募集少量资金来支持开发团队。与早期的互联网协议一样，目前还没有正式的程序来做出超过大致共识的决定。

## B.共识协议的稳定性

假设对交易有效性规则达成共识，已经进行了各种尝试来描述共识协议的性质，其必须使区块链被认为是稳定的。 我们将各种分析[46],[64],[84],[90]提出的属性系统化为五个基本的稳定性质。 请注意，不同的作者给出了不同的名称和不同的技术定义，我们在这里只给出一个非正式的概述。

* **最终共识。**在任何时候，所有符合规范的节点都将同意预先确定最终有效的区块链。 我们不能要求任何时候最长的链条完全是最终区块链的前缀，因为区块可能会因为临时叉子而被丢弃（变成“陈旧”）。
* **指数收敛。**深度为n的叉的概率是O（2-n）。这使得用户们高度信任，一个简单的“k确认”规则将确保他们的交易永久包含在高度的信任之中。
* **活跃度。**新的区块将继续添加，并在合理的时间内在区块链中会包含有效的交易。这些交易包含有适当的费用。
* **正确性。**在最长的链中的所有区块中包含有效的交易。
* **公平性。**按照期望，总计算能力为α的矿工将挖掘一定比例大约α的块（假设他们选择有效的块）。

如果所有这些属性都成立，我们可以说系统是稳定的，但并不清楚所有这些都是必需的。 货币的使用者可能对公平财产漠不关心，但这种财产往往被认为是持有的，在不存在的情况下，许多矿工可能会停止参与，最终可能会威胁到其他稳定的财产。

活跃度可能是最难定义的属性，而且我们的知识没有引人注目的正式定义。 显然，我们希望有人愿意支付能够使用网络，但不清楚交易成本和包含时间方面的确切要求是否合理。 严格的活跃度也意味着反审查的财产，这可能不是一些需要甚至是可取的，虽然这也经常被认为是比特币的核心属性。

令人惊讶的是，实际货币并不需要正确性，因为参与者可以简单的忽略最长链中的任何无效交易。 然而，正确性能够以SPV客户的形式获得重要的绩效优势，即只验证工作证明量而不是交易（参见第IV-A节）。

**激励相容性和博弈论。**中本聪最初认为，只要所有的矿工都遵循自己的经济激励措施，比特币就会保持稳定[90]，这个属性叫做激励相容性。激励兼容性从未在比特币或加密货币的背景下正式定义过;其流行作为一个术语可能源于其直观的吸引力和市场价值。我们可以考虑遵守默认采矿规则的合规[[13]](#footnote-13)矿工（见第II-B2部分）。在博弈论的术语中，如果普遍遵从性被证明是纳什均衡，那么这就意味着比特币的激励兼容性，因为没有矿工会有任何激励来单方面地改变策略。如果存在其他均衡，这意味着一个缺乏稳定的概念，如果普遍遵守是唯一的平衡，那么这个概念就具有很强的稳定性。另一方面，如果不合规策略主导合规性，我们必须问是否由此产生的策略均衡导致共识协议的稳定性。

1）比特币计价效用的稳定性：假设矿工的目标是纯粹获得比特币，我们讨论关于比特币稳定性的已知结果。

**简单的多数人原则可能不公平。**一个有趣的不符合规定的“采矿”策略是扣块攻击 [11], [45], [46],[[14]](#footnote-14)。如果“矿工”在最长的众所周知的区块链之前发现了两个区块，那么它可以有效地排除对方，直到网络的其余部分在一个区块内赶上，在此时可以发布保留区块。对于至少控制“采矿”能力1/3以上的“矿工”来说，这种策略主导了合规性，因为在对合规的“采矿者”采用这种策略时，“采矿”奖励的预期份额更高。取决于“矿工”在接近同时宣布的块之间如何选择，具有较低“采矿”能力的攻击者也可能是有利的。具有特权网络位置的攻击者可能能够比竞争对手更快地公布其保留区块，表明稳定性本质上依赖于关于通信网络的假设。

虽然这些结果表明普遍的承诺并不是许多采矿能力分配（包括在实践中观察到的）的纳什均衡，但是没有证据表明扣块攻击发生了，而且仍然不清楚是否存在可行的均衡策略解决扣块攻击问题。 如果扣块攻击发生了，这会损害公平。

**大多数遵守原则是一个完美的信息平衡。**Kroll等人[64]分析了一个简化的模型，其中矿工有关于所有已发现区块的完整信息（排除任何扣留区块）。在这个模型中，普遍遵守是纳什均衡的（虽然不是唯一的），这意味着比特币（虽然这种稳定很脆弱脆弱）是稳定的。

**多数遵守意味着趋同，共识和活跃。**可以看出，随着大多数矿工的顺从行事，一条最长（正确）的区块链将迅速出​​现。最初的比特币论文[90]创造了一个恶意的矿工的模型，试图通过“尝试产生一个比诚实链更快的替代链”来扭转交易，作为随机二项式游走，并且表明攻击者最终将会失去“竞争”其余的网络。Miller和LaViola [84]和Garay等[46]提供了更详细的形式证明，即如果大多数矿工遵守合规战略，沟通延迟相对于发现矿区的预期时间较短，矿工们最终会就不断增长的交易历史前景达成一致，而不管不合规的采矿者的策略如何。这足以确保除公平之外的所有稳定性（由于潜在的暂时扣留），“大多数”的确切数目取决于网络和其他假设。

**对于大多数的矿工来说，稳定性是不能保证的。**众所周知，控制大多数计算能力的单个不合规矿工就有可能通过收集挖矿奖励来破坏公平性，而不合规矿工要做到这些只需要无视他人发现的区块并且创建自己的区块链，这个区块链通过假设会变为最长的区块链。大多数矿工可以通过拒绝接受这些交易并任意审查交易的方式单独选择来破坏活跃性，并且如果它们出现在任何其他块中，则可以分叉。 最后，大多数矿工可能通过在区块链中引入任意长的分叉来破坏趋同和最终的共识，有可能消除“双花”（double-spend）交易的利润。 所有这些策略都会导致虚设的利润，但是由于这些行为是可以检测到的，所以这些策略可能不符合合理的矿工的长期利益。 我们将在下一节提到这一点。

**如果矿工能够勾结串通，那么稳定性是未知的。**即使在没有大多数矿工的情况下，小部分矿工也可能串通合作控制大部分的挖矿能力并且模仿任何大多数矿工做出的策略。目前还不知道这样的合作是否内部稳定，成员是否会受到诱惑，或被排除在外的矿工是否可以通过提供更有利的条件形成替代合作串通来解决问题。矿池可能成为合作串通的技术机制;矿工对矿池的选择和矿工在矿池之间迁移的行为尚未进行研究。 对于矿工是否会鼓励他人通过支付方式参与合作串通以及矿工如何通过支付方式参与合作串通，似乎也没有进行严谨的分析。

**矿业奖励下降的原因并不在于稳定性。**所有这些结果都用了一个简单的模型，即每个区块包含一个固定的比特币奖励数额。矿工收入从区块奖励到交易手续费将否定这种假设并且需要更多的复杂模型，这种复杂的模型需要考虑到交易手续费的分配。据我们所知，在最终没有挖矿奖励的情况下或着在中间情况下，稳定性将会受到如何的影响，目前还没有透彻的分析。因此，交易手续费成为了一个不可忽视的收入来源。

2）具有外部计价好处的稳定性

由于缺乏可观察的黑客攻击（尽管可能存在大规模矿池由不符合规定的行为来获利），比特币计价实用模型的结果并不能够说明判断比特币在实践中具有明显的稳定性（更不用说保证其在未来的持续稳定性），事实上，矿工们显然不是仅对比特币感兴趣，而是对获得现实利润感兴趣。 对此进行建模需要为矿工开发一种效用函数，不仅包括他们赚取的比特币的数量，还包括他们如何有效地将比特币转换为现实价值或其他货币。 矿工的策略可能会影响他们将比特币的财富转换为现实世界价值的能力，原因有三个：

**流动性限制。**目前，已外币交易比特币的交易所通常流动性较差。因此，攻击者可能获得大量的比特币，但无法将其全部转换为外部价值，或者只能以大幅降低的汇率来实现。

**面对黑客攻击时的兑换率情况。**一些违规的策略，特别是那些会以可见的方式影响稳定性的策略，可能会破坏公众的信心，从而削弱在短期内对比特币的需求。 实际上，在实践中，面对技术故障，汇率已经被发现下降了[72]。 一个很快就能赚取大量比特币的策略，一旦被发现就可能导致汇率崩溃，因此在汇率可以反应之前难以兑现，特别是考虑到上述流动性限制。

**比特币计价挖矿的长期赌注。**大多数矿工对维持比特币汇率的兴趣更大，因为他们将非流动性挖矿硬件中的重要资本捆绑在一起，如果汇率下降，比特币就会减少价值。如果矿工们希望他们能够在边际成本低的情况下保持他们在未来的挖矿能力份额（例如：如果他们的大部分硬件设施是提前支付的），那么他们可能会规避赚取更多比特币却降低降低挖矿奖励的预期价值的策略。请注意，这是一个限制因素，只要没有一个有效的市场，矿商可以出售预期的未来挖矿能力，即使矿工可以以比公众更快的速度提取被盗的比特币。

中本聪概括了这个论点的一个版本[90]来淡化大多数矿工攻击的可能性，他认为他们会永久性地损害这个系统（和汇率），随着时间的推移，按规则行事（遵循一个合规策略）会更加有利可图。在实践中，2014年7月，GHash.IO矿池在网络计算能力上超过了50％，公开承诺将来限制其能力，以避免损害系统的信心。

不幸的是，由于汇率在本质上取决于人的判断力和市场的信心，难以用易于理解的博弈模型来反映。 更正式地模拟汇率和实际效用函数的影响是一个重要的开放问题。

3）除挖矿收入之外的其他激励措施的稳定性：上文至少分析了两种策略，这些策略对于矿工而言可能是有利的，而矿工的效用并非纯粹来源于挖矿奖励。

**金手指攻击。**如果多数矿工的目标是明确地破坏比特币的稳定性，并因此将其作为货币的效用，他们可以很容易地做到这一点。Kroll等人[64]介绍了这个模型，并将其命名为金手指攻击。例如，一个希望破坏比特币以避免与本国货币竞争的国家，或者一个投入货币竞争激烈的国家，可能会动机尝试这种攻击。 可以说，这些袭击事件已经通过比特股得到了观察，在这种袭击中，比特币矿工成功地进行了低挖矿能力的新竞争货币的深度攻击[[15]](#footnote-15)。如果一个成熟的期货市场出现，矿工可以在短期对比特币汇率采取重大的行动，那么金手指式的攻击可能是直接获益的。

**羽毛分叉。** Miller[82]提出了羽毛分流的策略，在这种策略中，矿工试图通过公开承诺，如果黑名单交易包含在区块链中，攻击者将通过忽略包含目标交易的区块来进行报复 并试图分割区块链。 攻击者的分支将继续，直到它超越主分支并获胜，或者落后于k个分块，攻击者在这一点将允许发布目标交易。 一个拥有α<50％的采矿权的攻击者将会按照预期损失金钱，但是会成功阻止一个具有正面概率的黑名单交易。

然而，如果攻击者能够令人信服地表明他们认真对待报复性分岔，那么其他矿工就会回避目标交易，因为如果攻击者报复，他们也会失去期望。 因此，只要所有其他矿工相信攻击者在进行测试后会执行昂贵的羽毛分岔报复，攻击者也许能够无需成本执行黑名单。

## C.矿池的稳定性

矿池依赖于参与者发现有效区块，并自愿接受参与者提交部分股份以换取报酬，但扣押有效区块来降低该池的利润率。尽管这次攻击早已为人所知，但是扣压有效区块降低自己的收入似乎是自我破坏的。然而，已经表明[33]，一个大型挖矿者（或池）实际上能够利用部分挖矿能力并提供部分获利份额来渗透其他矿池从而获利，而不是利用它来扣压有效区块。好处是，用于渗透的能力不会增加挖掘难题的难度（因为区块尚未公布），但仍然可以获得利润。 这个策略对于一个大型矿工或矿池来说是非常有利的，因为攻击者和侵略性矿池都有一系列的挖掘能力。

Eyal[44]提供了对这种攻击的扩展处理，并且表明在任何两个池之间，所得到的结果是一个迭代的囚徒困境，两个池的纳什均衡的攻击，而不是攻击的帕累托均衡。 如果大规模进行，这种攻击可以被统计检测到，这在2014年6月Eligius池中至少发生过一次[124]。 但是，聪明的攻击者可以使用许多参与者地址轻松地混淆攻击。 已经提出了进一步的对策，但没有认真研究或部署。 作为反复囚徒困境，矿池之间有可能会通过渠道外沟通和报复的威胁来避免相互攻击。

## D.点对点的稳定性

几乎所有对比特币的分析都假设，对等层的功能如同规定，一般来说，大多数参与者将在合理的时间尺度内学习几乎所有可用的协议状态信息。 但是，Babaioff等人 [8]表明，在点对点层的信息传播并不总是激励兼容的。 参与者是否将对等网络的足够价值内化为公共利益以证明传播信息的机会成本是未知的，Babaioff等人观察到的信息传播平衡（人们是否愿意参与对等协议）是不稳定的，并最终可能会被打破。

Johnson等人[59]，[68]研究对等协议的参与者是否以及何时激励参与者对他人的网络级拒绝服务攻击。他们得出结论认为，矿池有攻击的动机，较大的池比小池更好地攻击，较大的池比小池有更大的动机来攻击。 因为定期对池的拒绝服务攻击进行观察，所以这个理论分析可以通过观察现象学来支持[120]。 其他人进行了测量和模拟研究，以确定信息传播的动态和时间尺度[38]，[40]。

# 客户端的安全性

比特币的受欢迎程度使可用和安全的密钥管理对于大量的新用户群体来说非常重要。 与许多其他密码应用程序不同，如果密钥丢失或被泄露，用户将遭受即时和不可撤销的经济损失。 因此，它是在安全性研究中一个令人兴奋和重要的领域。

## A．简化支付验证（SPV）安全

虽然比特币客户端会维护整个区块的有效副本，但这会给手机等移动设备带来极大的负担。一个简单的观察导致了一个选择：假设大多数节点只在有效链上挖矿（III-B节的正确性），那么客户端只需要验证工作量证明，并且可以相信最长的链只包含有效的交易。 这样的SPV证明[90]使得不受信任的节点能够向小型客户有效地证明交易已经被包括在商定的历史中。

SPV是在大多数比特币移动客户端的基础上的BitcoinJ库中实现的。SPV验证需要处理不断增长的工作量证明区块链，尽管优化是可能的，例如从硬编码检查点开始。SPV也关心隐私，因为它要求披露客户感兴趣的第三方的一系列地址（参考第七部分和第四十九部分）。

## B．密匙管理

比特币依靠公钥加密技术进行用户认证，而今天几乎所有其他形式的在线商务都依赖于密码或者保密的信用卡信息。 比特币软件的开发者试图通过各种方法来解决，或者至少掩盖长期存在的可用性问题和关键性的存储和管理问题。Eskandari 等人[43]提出了一套比特币密钥管理接口的可用性评估标准，并得出结论，目前的工具采用复杂的“隐喻”，不能完全捕捉关键管理行动的影响。

**存储在设备上的密钥。**直接在磁盘上存储密钥池是最简单的模式，但密钥可能被特定制作的恶意软件窃取[75]。有些客户端会将更改发送到新创建的比特币地址，每次当前密钥池耗尽时（通常在没有任何用户界面指示的情况下），都需要新的备份，而其他客户端会将更改发送到始发地址，或者从单个地址派生所有随机密钥种子。

**分割控制。**为了增强安全性并且避免单点故障，比特币可以使用指定n个公钥的k-n多重签名脚本进行存储。 对于要赎回的脚本，必须从这n个公钥中提供k个有效的签名。 一个简单的例子就是在发送资金之前需要用户的笔记本电脑和手机的认证。 另外，资金可以存储在一个单一的公共密钥下，但是这个密钥的份额可以在n个参与方之间使用门限密码[50]进行分配。 阈值签名实现了相同的k-n安全性，但看起来像区块链上的普通付费到发布—密钥—哈希交易，并保持参数k和n是私有的。

**密匙保护的钱包。**比特币客户端可以允许使用从用户选择的密码派生的密钥对存储的密钥池文件（称为钱包）进行加密。 密码保护的钱包可以阻止某些类型的盗窃行为，如果文件被物理或数字盗取，还需要密码猜测或按键捕获。 密码保护的钱包可能会误导用户认为密码本身提供了访问他们在新设备上的资金。

**密码派生的钱包。**密钥池可以确定性地从单个用户选择的秘密获得，如果秘密致力于记忆（这种方法通常被称为脑袋），则允许跨设备使用。 无限制的穷举密码搜索是可能的 - 彩虹表已经在区块链上发现了不适当的保护比特币地址。 另外，密码遗忘会使所有相关的资金无法恢复。

**存储空间。**存储在被动便携式媒体（例如纸质或者U盘）中的钱包增强了面对恶意软件威胁的防盗保护，并提供了一种熟悉的实际安全性的构思模型。但是，由于密钥池已经耗尽，所以必须更新它们。 对于纸质钱包，可以通过被动观察钱包（例如在电视直播[101]上）以可扫描形式（例如QR码）打印的密钥被盗。 最后，钱包必须最终将密钥加载到要使用的设备中，在那时变得容易受到恶意软件的影响。

**气隙和硬件存储。**气隙存储是存储密钥的一种特殊情况，持有密钥的设备可以执行计算，例如为其所持有的密钥签名交易。 通过将钥匙直接暴露在连接互联网的设备上，空隙设备可以阻止某些类型的盗窃行为。 也就是说，未经授权的访问事务签名预告与自动访问关键字没有多大区别。硬件安全模块（HSM）通过将密钥材料与主机设备隔离开来，只显示签署事务的能力，从而模拟气隙的属性。

**托管钱包。**第三方Web服务通过标准的Web验证机制（如密码或双重身份验证）提供密钥存储，管理和事务功能。这提供了传统网上银行最接近的经验，但它需要信任主机。 已经记录了很多被托管钱包盗窃[41]或破产[86]的事件，其中包括超过40起涉及损失超过1000比特币的事件。

# 比特币的完善

我们现在把注意力转向比特币修改和扩展。 在本文的其余部分中，我们将评估和比较提议的变更，在本节中，我们将讨论实施变更的可用机制。

## A.比特币自身的升级

我们可以区分一下变化的级别：

* **硬分叉。**协议的变化需要一个硬分叉，如果它承认在前面的规则下被认为是无效的事务或块有效，例如增加块奖励，改变固定的块大小限制或添加新的操作码。 如果矿工更新到新的协议，他们可能会产生被其他节点拒绝导致永久性（因此是“硬”）叉的块。因此涉及硬分叉的变化因此需要在实践中尝试近乎一致。
* **软分叉。**与硬分叉相比，软分叉变化更是向后兼容现有客户的软分叉变更。通常这涉及限制哪些块或交易被认为是有效的。这样的改变只需要大多数矿工的支持来升级，因为老客户将继续考虑他们的区块是有效的。没有升级的矿工可能会浪费计算工作，其余的网络认为无效和忽略，但总是会重新加入大多数矿工发现的最长的链条。这使得软分叉的变化比硬分叉更为安全。在某些情况下，可以使用软分叉将新的操作码引入脚本语言。这是可能的，因为目前有几个未使用的操作码被解释为空操作;包括交易输出中的这些信息可能会使任何人都花钱，因此通常会避免它们。然而，如果矿工决定拒绝这个操作码所指示的一些条件失败的交易，那么这些操作码中的任何一个都可以被赋予新的语义。可以接受的交易范围严格缩小，因此只需要一个软分叉就可以加强效果。回想起来，将所有未使用的操作码定义为空操作将是明智的，这通过软分叉提供了最大的灵活性来引入新的变化。
* **传播策略更新。**回想一下第II-B3节，节点强化实施更严格的策略，而不是实施实际接受的有效策略。 改变这个策略或通信网络的大多数其他方面需要最少的协调，因为它们通常可以以向后兼容的方式完成，节点通告它们的协议版本号。 默认传播策略已经多次更改，以添加新的标准事务类型，如多重签名事务。

## B．山寨币

由于可以改变比特币的限制而没有硬分叉，数以百计的衍生系统，被称为山寨币，山寨币已经出现了可替代的设计方法。 尽管一些系统（如Ripple）是完全独立的设计，但这些系统中的很多都包含了比特币的代码库，并保留了大部分功能。山寨必须引导货币的初始分配以吸引用户参与，这可以通过几种方式实现：

* **新的创世区块。**山寨币可能只是从头开始一个新的区块链，像比特币早期那样为初始矿工分配资金。由于创始人希望通过早期开采获得现金而发起的一轮山寨币，这种方法现在被加密货币社区看得很仔细。[[16]](#footnote-16)
* **分叉比特币。** 为了避免其创始人的特权，一个山寨币可能会故意选择在某个时候分叉比特币，接受之前的交易历史和资金所有权。 比特币所有者将在原始系统中继续使用比特币，并在创建时加上相同数量的新货币。 从技术上讲，这将像硬分叉一样运作，只是没有声称叉是合法的比特币区块链。 有趣的是，这种做法似乎没有被认真地尝试过。
* **“燃烧证明”。**比较流行的比特币分配方法是“燃烧证明”[113]，其中用户必须可证明地销毁一定数量的比特币，通常通过将比特币中的资金转移到一个特殊的地址，其私钥不能被找到，比如密钥全零的散列。 这种做法有永久性降低流通中比特币数量。
* **挂钩侧链。**最近，一些有影响力的比特币开发者[9]提出了侧链，比特币可以被转移并最终被赎回。 添加验证规则来从侧链赎回货币将需要至少一个比特币软分叉。

山寨币也必须与比特币竞争矿工（并避免比特币矿工的金手指攻击），在货币实现非零汇率之前，这可能是困难的。 一个流行的方法是合并挖掘，即如果根币被包含在有效的比特币区块中，则山寨币接受区块，从而使比特币矿工能够在没有执行任何额外工作的情况下挖掘山寨币中的区块。 这可以快速提供给山寨币整个比特币的挖掘力量，因为许多比特币矿工现在合并挖矿，大量山寨币获得额外的奖励。 无论如何，它排解了山寨币的计算难题。

# 可替代的共识协议

比特币的共识协议一直是其中争议最大的组件，因为有关稳定性的问题（参见第III-B节），对协议性能和可伸缩性的担忧[112]，以及关于其计算难题浪费资源的担忧。 在本节中，我们评估备选方案以达成一致意见，并指出在每种情况下，拟议变更的稳定性影响都是未知的，替代方案很少鉴定它们声称提供的任何特定稳定的属性。

通常情况下，尽管考虑到缺乏确保比特币本身稳定性的稳固模型，但是交替共识方案的目的是为了找出一些特定的比特币问题，并希望比特币的稳定性能够继续下去，

## A．参数更改

比特币的共识协议包含了很多“魔术常数”，这些“魔术常数”是在最初的猜测基础上进行硬编码的。 几乎所有的币种都至少有一些这样的参数，但是这些修改往往是有争议的，我们对于如何选择这些参数以及它们如何影响稳定性只有较少明确的指导方针。

**区块间时间和难度调整窗口。**比特币会自动调整计算难题的难度，以便相隔十分钟找到解决方案。 此设置主要受网络延迟的限制; 如果解决方案的速度太快，那么矿工会频繁地找到冗余的区块，然后才能传播。 另一方面，较慢的数据块速率直接增加了用户需要等待事务确认的时间。 比特币的设置主要受网络延迟的限制; 所有我们知道的山寨币具有相同的速度或更快（Litecoin，第二个最流行的系统，速度快四倍）。 有许多建议修改通信网络的各个方面以减少延迟，使得这个参数能够被安全地减少[38]，[73]，[112]。

**限制区块和交易信息的大小。**其中一个最有争议的提议的变化是增加块的大小1MB的限制[3]。随着交易量继续稳步增长，这个限额可能会很快达到。交易量的上限目前只有每秒7个，比Visa网络的峰值容量小约1000倍[53]。一旦达到这个限制，交易将有效地使用他们的费用来投标稀缺资源。这可能会增加使用比特币的成本，可能会减缓采用率，但会增加矿工的收入。这也可能导致用户依靠中介机构来进行汇总和结算交易。限制是人为的，网络的带宽可能会持续增长;另一方面，增加的交易量可能会排除一些带宽受限的参与者。虽然据我们所知，几种山寨币已经提出了这个限制的规范，但我们并没有实际利用这个能力，所以它不知道它将如何影响系统的运行。

**货币政策。**比特币的一致性议定书通过新币的兑换率和兑换率的变化来有效地制定货币政策。 通过规定限制货币数量，比特币实际上有一个定义的货币政策，这导致多个经济学家预测这个系统最终将会被没有人愿意花费比特币而囤积比特币的行为而松动 [52] ，[65]。 数字货币的发行量是最广泛变化的参数之一：例如，在Dogecoin中通货膨胀将继续无限期地以一个和谐的速度减速，而在Freicoin[116]中通货膨胀率永远保持不变。

## B．可替代的计算难题

Miller等人 [85]提出了形式上的比较兼容的工作证明方案，这种方法被称为刮擦谜题，它基本上必须分解成单独的尝试。 这个属性通常被称为“无进展”的谜题。这保证了每个区块的创建者都是通过计算能力的加权随机样本来选择的，即使是小的参与者也能够获得他们贡献的（比例）奖励， 连续难题解决方案之间的时间足够大，难题解决方案会传播。 无进展性是必要的，但不足以实现公平协议。 比特币的SHA-256难题是无进展的，但许多其他的创新是可能的。

**ASIC抗性难题。**虽然比特币挖矿最初是使用通用处理器进行的，但挖矿的竞赛导致了朝着更强大，更节能的定制硬件的稳步发展。 今天，ASIC占比特币大部分的计算能力。 泰勒就大规模计算SHA-256的技术挑战提供了一个很好的调查，并估计今天的ASIC已经处于理论效率极限的同一个数量级[115]。

由于大多数参与者都不拥有ASIC，所以根本不会把挖矿行为从核心民主价值（比如“oneCPU-one-vote”[90]）中移走，因为这样做会带来负面影响。 提出了许多针对ASIC的挖掘难题的建议。 理想情况下，使用商用硬件可以有效解决抗ASIC的难题，而定制硬件的性能仅有微小的提升。 到目前为止所采用的主要方法是设计“内存紧张”的谜题，其目的是要求有效访问大容量内存。 到目前为止，最流行的记忆难题（在Litecoin和Dogecoin等中使用）一直是脚本哈希函数[96]，最初是为了防止破解哈希密码而设计的。 到2014年，还不知道是否有可能设计一个难以计算的记忆难题。 Tromp的“杜鹃循环”难题[117]似乎很好地回答了这个问题。

如果可能出现ASIC阻抗问题，那么这仍然是一个重要的开放性问题。[[17]](#footnote-17)例如， ASIC的脚本已经在市场上发布，并且性能提升与SHA-256 ASIC相当。 这也是不明确的，性是可取的.ASIC意味着从商品设备窃取周期的网络不再与先进挖矿设备竞争[57]。 正如第III-B2部分所讨论的那样，依赖于比特币未来采矿奖励来收回专用ASIC投资而没有其他价值的大型矿工也可能具有更强的抵制作用。

**有益的难题。**通过计算难题达成共识似乎在计算能耗和用于制造采矿设备的能源和资源方面都是浪费的。 如果有可能获得相同的安全等级，同时利用这项工作来达到一些额外的目的，那么这些废物中的一部分可以被回收。 Berker等人 [14]也认为，比特币最终可能会被世界能源供应商所主宰。

一个常见的建议是使用搜索功能与科学研究的应用程序，如流行的Folding @ Home [67]项目。 对于有用的难题来说，一个挑战就是它们必须被自动生成，并且没有可信任的各方组织进行验证，否则这个组织可以选择已经有了头绪的难题。 Kroll等人 [64]进一步认为，任何有用的难题都必须产生一个纯粹的公共物品，否则它可能会增加挖掘的数量，从而消除任何回收效果。

质数币第一个在运算难题中引入了有用的难题。它的难题是需要寻找大素数序列，并且可能被用作密码协议的参数。 Miller等人 [83]提出了一个结合了证明可回收性的谜题，因此挖掘需要存储一部分大型公共数据集。 特别是，如果公共数据集对于比特币网络本身（例如区块链历史）是有用的，则这种方法提供额外的激励来为网络贡献资源。

**Nonoutsourceable难题。** 大型矿池的发展[78]促进勾结和合作形成的潜力促使了难以外包的难题的设计。 一个矿池的成员本质上并不相互信任; 但是，这些联盟是成功的，因为成员可以很容易地证明他们正在进行挖矿工作，如果成功的话，他们会向池库经理支付报酬。 Miller等人 [85]以及Sirer和Eyal [111]提出了“无法通过资源”的谜题，以确保谁执行挖矿工作谁可以要求自己的奖励，当一个区块被发现，从而阻碍矿池的执法机制，并在匿名参与者之间不太可能形成大型矿池。

## C．虚拟挖矿与工作量证明

在较高层次上，需要花费较多的资源来进行挖矿的工作量证明。与其让参与者通过交换他们的财富来获取计算资源（然后交换采矿奖励），他们可能仅仅是让他们直接交换财富来选择区块。 随机样本是通过计算能力加权的参与者的随机样本而不是通过推进全球历史，而是通过当前的财富分配进行加权。 我们可以称这种方法为虚拟挖掘。 它有时也被称为“证明权益”[98]。

虚拟挖矿提供了两个主要的好处：首先，攻击者获取足够大的数字货币可能比获取足够强大的计算设备更困难。 其次，通过避免真实资源（即计算周期）的消耗，不会浪费现实世界的资源。 到目前为止，已经有几种虚拟矿业的变化，主要是因为拥有一定数量的货币使得有资格选择下一个区块的标准不同：

* **数字货币年龄验证。**点点币 [63]提出通过发布交易（可能是为了自己，在这种情况下硬币不会丢失）来证明拥有一定数量的货币。 每一种货币的数量都是根据它自上次移动硬币以来的时间来计算的。
* **存款验证。**在Tendermint 算法中[66]中，参与挖矿需要在一个时间锁定的债券账户中存入硬币，在这期间这些比特币不能移动。
* **“燃烧”验证。**Stewart[113]提出了销毁硬币（把它们发送到一个不可靠的地址）的方法。
* **活动证明。**Bentov等人[20]提出，每个比特币所有者默进入“挖矿彩票”; 周期性地，（例如，从网络上发生的交易产生的）来自信标的随机值被用于在系统中的所有比特币中随机选择; 获胜比特币的当前所有者必须在一段时间间隔内用签名消息作出回应。

还没有任何形式的假设模型可以允许比特币挖矿系统实现安全，或比较比特币挖矿系统和通用环境中的计算难题。 Poelstra [97]对大众的观点进行了一项调查，认为消耗外部资源（即消耗电能）是区块链安全所必需的，因此虚拟挖矿方案本质上是不可行的。 中心论点 - 被认为是无关紧要的问题 - 是虚拟挖掘容易受到无谓的模拟攻击; 建立货币分配不同的历史交替观点是没有任何意义的。 针对虚拟开采的稳定性提供严格的论点仍然是一个悬而未决的问题。

## D．指定的当局

虽然比特币的去中心化已经被证明是一个有效的卖点，并且在社区中被许多人所保护，但是如果我们能够依靠小部分指定机构来接收，依次订购和签署交易，那么共识就会变得非常简单。 这将使得稳定性假设更容易推理，并且一次性消除对浪费计算的担忧。 劳里[69]首先提出使用指定的权威名单和一个标准的拜占庭协议。

类似于大型比特币矿工由于未来汇率的利益而未被激励攻击的情况，如果当局通过诚实行事赚取小额收入，他们就不会有任何行为失误的动机。 类似的选择可用于分配新的资金，用于证明解决方案（Laurie最初的建议是[69]当局抽签）。 通过使用互不信任的权威机构[69]，来利用社交网络来选择信任的机构[108]，或者授权硬币所有者在每次花钱时选择可信赖的机构[24]，这些机构的信任可能会进一步受到限制。 Ripple [108]是与这个模型一起使用的少数山寨币之一; 然而，其稳定性论点基本上还没有得到证实。

# 匿名与隐私

比特币提供了一种有限的不可链接性：用户可以随时创建新的假名（地址）。这在最初的规定中被认为是提供了强大的隐私[90]，然而人们很快就清楚地认识到，由于区块链的公共性质，有时可以追踪假名之间的货币流量而获取用户信息。

## A．匿名化

不相关的实际水平在很大程度上取决于实施细节，我们称之为使用习惯用法[80]。 例如，为每次销售生成新付款地址的商家确保收到的付款不会自动链接到区块链上。 相比之下，客户可能需要从她拥有的多个地址汇集支付金额，[[18]](#footnote-18)将这些地址（及其伴随的交易历史）连接在区块链上，因为不同的用户很少为单个联合交易贡献投入[[19]](#footnote-19)其他 “每一个非变化的输出由一个单一的实体控制”[4]和“一个地址最多只用一次作为变化”的习语[80]也可以被攻击者用来把其控制的不同地址链接在一起。

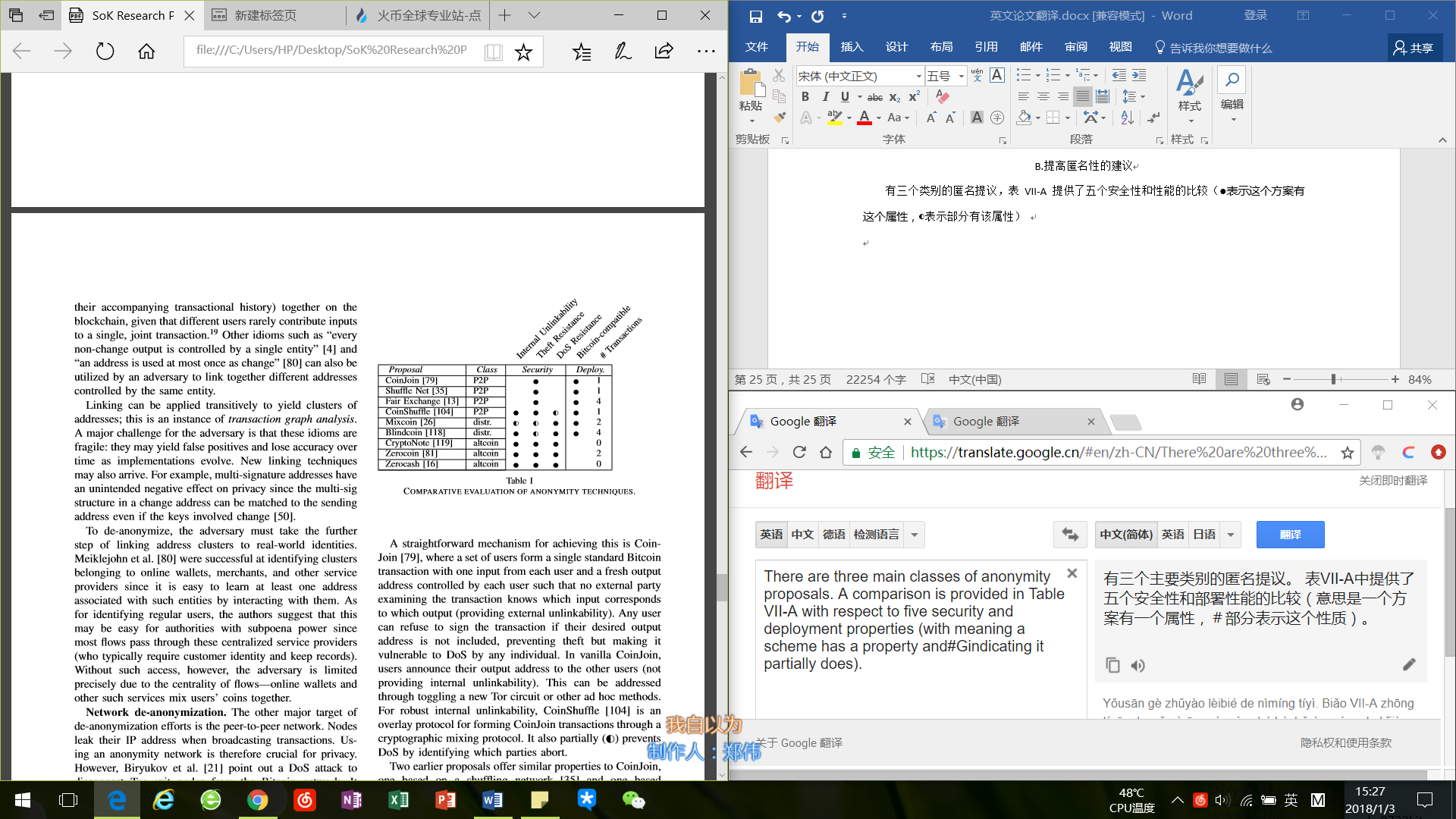
链接可以被传递地应用以产生地址簇; 这是交易图分析的一个实例。 对手的一个主要挑战是这些成语是脆弱的：随着时间的推移，它们可能会产生误报，并随时间推移而失去准确性。 新的链接技术也可能到达。 例如，多重签名地址对隐私有负面影响，因为即使所涉及的密钥发生变化，变更地址中的多信号结构也可以与发送地址相匹配[50]。

为了消除匿名，攻击者必须采取进一步的步骤，将地址簇链接到真实世界的身份。 Meiklejohn等人[80]成功地识别属于在线钱包，商家和其他服务提供商的集群，因为通过与这些实体交互来学习至少一个地址是容易的。 至于识别普通用户，作者提出，这可能很容易传递权力，因为大多数交易过程都通过这些集中服务提供商（谁通常需要客户身份和保持记录）。 但是，如果没有这样的访问权限，攻击者就会因流量的中心性而受到限制 - 在线钱包和其他此类服务将用户的硬币混合在一起。

网络去匿名化。去匿名化工作的另一个主要目标是点对点网络。 广播交易时，节点泄漏其IP地址。 因此使用匿名网络对于隐私至关重要。 然而，Biryukov等。 [21]指出DoS攻击将Tor出口节点从Bitcoin网络中断开。 比特币的P2P层会不断发展，以更好地利用Tor或者开发一个专门的匿名网络。 最后，由于私人检索客户感兴趣的交易清单的困难，目前的SPV实施提供了很弱的隐私性[49]。

## B.提高匿名性的建议

有三个类别的匿名提议，表VII-A提供了五个安全性和性能的比较（●表示这个方案有这个属性，◐表示部分有该属性）

点对点。在P2P混合协议中，一组比特币持有者共同创建了一系列（私下）排列硬币所有权的交易，使得每个参与者都是匿名的。 这个过程可以在不同的用户之间重复以增加匿名集合数量。

实现这一点的直接机制是CoinJoin [79]，其中一组用户形成一个标准的比特币交易，每个用户输入一个输入，每个用户控制一个新的输出地址，使得没有外部审查交易的人知道哪个输入对应于哪个输出（外部不可链接性）。任何用户可以拒绝签署交易，如果他们所需的输出地址不包括在内，防止盗窃，但容易受到个人的DoS攻击。 在CoinJoin中，用户向其他用户公布其输出地址（不提供内部不可链接性）。 这可以通过切换新的Tor电路或其他临时方法来解决。 为了强大的内部不可链接性，CoinShuffle[104]是一种覆盖协议，用于通过密码混合协议形成CoinJoin交易。 它也部分地（◐）通过识别哪些方中止来防止DoS。

早期的两个提案提供了与CoinJoin类似的特性，一个基于一个回收网络[35]，另一个基于公平交换[13]。 然而，这两者都限于双面混合，使内部不可链接性成为可能。 为了解决双方混合协议寻找合作伙伴的困难，Xim [22]是一个寻找混合伙伴的分散协议，使用支付给矿工的三个阶段的费用来阻止拒绝服务攻击。

**分布式混合网络。**在Mixcoin [26]中，用户向第三方组合发送标准尺寸的交易，并从相同组合的其他用户提交的硬币中接收相同的金额。 这提供了匿名对外部实体和部分内部匿名（◐），因为混合将知道用户和输出之间的链接，但其他用户不会。 其他用户也不能破坏协议。 虽然混合可能会随时盗取比特币，但可以使用签署的权证（提供部分◐防盗功能）来识别作弊混合。 虽然Mixcoin的保证和其他功能尚未开始使用，但是这是最接近第三方混合的建议，也是最常用的实践[88]。

Blindcoin [118]使用与Chaum的原始电子现金提案类似的代币扩展了Mixcoin [28]。 这样可以防止一个诚实但好奇的组合学习输入和输出之间的映射，并升级到完全内部的不可链接性，但需要花费两个额外的交易来发布和赎回这些令牌。

**具有集成不可链接性的山寨币。**零币 [81]是一个具有整合不可链接性的提议的山寨币，使用比特币的基础货币和一种名为零币的匿名影子货币。 用户仅以基础货币进行交易，但是可以相对于所有的零售商集合（比上述其他技术设置更大的匿名集合）匿名地循环基础货币进出零售结果。 这提供了强大的不可链接性，没有盗窃或DoS问题，也不依赖除矿工以外的任何实体。 但是，它与比特币不兼容，必须作为一个山寨币（或硬分叉）来实现。 PinnochioCoin [37]是一个类似的建议，使用不同的密码结构。

Zerocash [16]对于一个匿名的山寨币是一个更强有力的建议。 Zerocash交易是一种称为SNARKs的特殊类型的零知识证明[17]，它根本不显示任何关于数量或收件人的信息（除可能的公共交易费用外），从而实现一个没有公开披露信息的完全无法追踪的分类账。 SNARK是迄今为止没有任何新密码，并且需要由可信方初始生成秘密参数; 然而，最近的工作表明，这种初始设置可以分布在一组互不信任的方面[18]。

CryptoNote [119]是一个使用环签名的密码混合协议，已经被用作几个隐私聚焦的山寨币的基础。 用户可以通过在他们选择的一组k个（可能是未使用的）硬币上提供一次性签名来发送一个硬币，其作为匿名集合起作用。一次性属性确保了双重支出的尝试可以相互链接，导致无效的交易。交易规模是线性的，单个交易的匿名集合的大小。该方案与Zerocoin或Zerocash相比具有较好的性能，但是有较弱的匿名性。

# 比特币功能的扩展

尽管比特币可以简单的描述为数字货币，但矿工实施脚本语言的能力使得两个或更多相互不信任的各方之间可能需要可信中介的许多其他类型的交互。 我们使用术语“非中介”来指代设计交易的一般过程，以消除对可信中介的需求。

## A．如今比特币的去中心化情况

比特币是一个可扩展平台的程度往往被夸大了。 脚本语言仍然受到高度限制。 但是，许多协议都是针对非中介化而设计的，这可以通过比特币当前的交易来实现。 我们确定了三种一般的非中介化策略：

**原子性。**在许多情况下，可以直接使用区块链提供的功能强制执行所需的安全属性，以及交易可以是原子的，在多方签名之前无效。 CoinJoin [79]就是一个简单的例子，没有参与者的硬币交换，直到各方签字。 另一个例子是Hearn的“连续微支付”协议[55]，它有效地使用了带外频道，允许一方批准几乎连续的缓慢释放资金，（例如：每秒一分钱）以换取一些计费服务，如互联网接入。 付款人可以在任何时候结束协议，通过停止签署更多的交易，在这一点上只有一个交易需要张贴到区块链。 另一个聪明的协议是Nolan的原子交叉链交换协议，它允许用户用两个链接的交易和原子安全性在两个山寨币之间交换货币[91]。

**抵押品。**在其他情况下，如果所需的安全财产不能直接执行，则比特币可以通过发布只有在正确行为的情况下才退还的存款或债券来提供可接受的补救措施。这种方法由Andrychowicz等人的多玩家彩票协议来例证。[5]。 N方中的每一方放置一个Bk下注，一方（随机选择）与BkN一起走开。 为了保证作弊的玩家不会通过先学习结果并有选择地放弃协议来破坏游戏，每个玩家必须存放BkN2。 如果任何参与者中止协议，他们会放弃其存款，这是用来补偿他人的最高金额，他们可以获得这些金额。 这种方法不限于抽奖，而是实际上可以为任意多方计算提供一个公平的概念[19]。

**可审计性。**即使比特币不被用来对不诚实的一方采取补救措施，它仍然可以在提供证实不诚实方的证据方面发挥关键作用。 其中一个例子是绿色地址[58]，其中拥有众所周知的公钥保证的支付处理器永远不会签署无效或冲突的交易。 从绿色地址接收交易的用户可以在等待它被包括在块中之前接受它（即做出不可撤销的决定）。 如果交易在某个时候被区块链上发布的冲突交易抢占，那么用户可以很容易地得到证明服务器被骗的证据。 Mixcoin使用了类似的技术[26]，其中不怎么可信任方提供签名保证，这些保证与区块链一起将提供无可辩驳的不当行为证据。

## B．比特币作为数据存储的作用

拓展比特币的另一种方法是将其仅用作任何人都可以编写的全局附加日志。

**时间戳的安全性。**由于区块链是（模型分叉）附加的，它可以立即作为一个安全的时间戳服务[31]，这是在各种安全协议中都很有用的。任意数据可以通过多种机制写入区块链——社区更喜欢使用一个小的，可证实的脚本，其中包含一个未使用的变量中的数据。[[20]](#footnote-20)多个服务器从用户收集数据，并将Merkle根发布到区块链，允许任何人通过时间戳编写任意数据。

**数字令牌：彩色硬币。**由于数据可以写入单个交易，因此可以用“颜色”来标记某些交易。这使得一个名为有色金币的协议[103]定义了一套规则（不是由矿工强制执行）将颜色从输入交易转移到输出交易。比特币最初可以通过包括来自任何被授权为某些应用发布颜色的机构的特殊签名来着色。这允许创建任意的令牌，可以彼此交易，也可以为普通的无色比特币交易。彩色硬币已被提出用于许多应用，例如交易股票或财产权。 由于比特币矿工不执行彩色硬币协议的规则，因此验证交易的颜色需要扫描区块链以查看所有先前交易（排除SPV证明）。

彩色硬币用区块链的历史追踪特点作为自己的功能。一般来说，据观察，每笔交易的产量都有独特的先前历史，这对于不同的用户都有其意义。这意味着从长远来看，比特币不能保证是交换的。

**覆盖协议：万事达币。**一个更灵活的方法是使用比特币的共识机制，但将完全不同的交易语法（具有任意的有效性规则）定义为区块链上的任意数据。请注意，这种设计消除了比特币的共识机制通常提供的正确性属性，因为比特币矿工不会了解新的交易类型。 因此，无效的覆盖交易可能会被公布，并且需要被覆盖系统中的参与者忽略。SPV证明也是不可能的，因为用户必须验证整个覆盖交易历史。 两个突出的系统是交易对手[39]和Mastercoin [123]，它们定义了大量用于交易数字资产和合同的附加交易类型。

## C．扩展比特币的交易

比特币脚本语言是故意添加限制的; 实际上，原始源代码包含了更通用的语言，但是大多数操作码被标记为不可用。 在我们论文[25]的完整在线版本中，我们解释和评估了诸如Namecoin [76]或Ethereum [125]等多种方案，以扩展比特币的功能，为非中介化提供更多元化的平台。

# 结束语

我们基于学术和（广泛、分散）在线文献对比特币进行了广泛的分析，这显示了设计实用加密货币的新想法，这也是计算机安全社区面临的一个长期挑战。创新不仅限于新的加密货币协议设计，而且涉及到计算机安全，分布式系统，硬件设计和经济学等诸多领域。 这是一个非常丰富和深刻的空间，不应该被忽略，因为很多想法不是来源于传统的计算机科学研究机构。

然而，虽然我们的知识有了长足的发展，但我们的理解往往还是缺乏。 一个简单的事实证明了这一点：鉴于有机会从头开始设计一个货币体系，不清楚比特币有什么重要的偏差是可取的，或者它们在实践中会产生什么样的影响。 这并不是说比特币是无暇的，因为它的许多设计怪癖表明。 还有几个领域，如匿名性问题，其中提出了明显优越的设计。 然而，对于基本的稳定性和效率，目前还不清楚是否可以设计一个替代比特币的去中心化共识系统。 文献甚至没有提供足够的工具来评估比特币本身在哪些经济和社会假设下将保持稳定。 同样，为了设计具有新功能的中介协议，目前还不清楚如何扩展比特币的功能，而不会破坏观察到的稳定性。

总的来说，我们根本没有一个具有足够预测能力的科学模型来回答关于比特币或相关系统如何在不同参数或不同情况下运行的问题。尽管偶尔有人对比特币社区学术计算机科学研究产生疑虑，但我们主张在研究中扮演重要角色，而不是简单地“让市场决定”。现在很难评估比特币的成功在多大程度上是由于其特定的设计选择，而不是其先发优势。

比特币是一种罕见的情况，这种情况下，实践似乎超越理论。我们认为研究界有巨大的机会来解决我们已经制定的关于比特币的许多开放性问题。

致谢

作者在此感谢以下同事对本文草稿的反馈意见：Sergio Demian Lerner，Luke Valenta，Albert Szmigielski，Gus Gutoski，Ben Laurie，Ittay Eyal以及IEEE安全与隐私的匿名审稿人以及比特币社区。Joseph Bonneau得到一个安全可用性奖学金的支持。 杰里米·克拉克（Jeremy Clark）得到了NSERC Discovery Grant的支持。Joshua A. Kroll得到了国家科学基金会研究生研究金项目DGE-1148900的支持。Arvind Narayanan得到了NSF Grant CNS-1421689的支持。

参考文献

[1] G. Andresen. March 2013 Chain Fork Post-Mortem. BIP 50.

[2] G. Andresen. Pay to Script Hash. BIP 16, 1 2012.

[3] G. Andresen. Blocksize Economics. bitcoinfoundation.org, October 2014.

[4] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In Financial Cryptography, 2013.

[5] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek. Secure Multiparty Computations on Bitcoin. In IEEE Symposium on Security and Privacy, 2014.

[6] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek. On the Malleability of Bitcoin Transactions. In Workshop on Bitcoin Research, 2015.

[7] J. Aspnes, C. Jackson, and A. Krishnamurthy. Exposing computationally-challenged Byzantine impostors. Technical report, Yale, 2005.

[8] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On Bitcoin and Red Balloons. In SIGecom Exchanges, pages 56–73. ACM, 2012.

[9] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Tim´on, and P. Wuille. Enabling blockchain innovations with pegged sidechains, 2014.

[10] A. Back et al. Hashcash-a denial of service counter-measure, 2002.

[11] L. Bahack. Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft). Technical Report abs/1312.7013, CoRR, 2013.

[12] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten. Have a snack, pay with Bitcoins. In IEEE P2P, 2013.

[13] S. Barber, X. Boyen, E. Shi, , and E. Uzun. Bitter to Better—How to Make Bitcoin a Better Currency. In Financial Cryptography, 2012.

[14] J. Becker, D. Breuker, T. Heide, J. Holler, H. Rauer, and R. B¨ohme. Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. In WEIS, 2012.

[15] M. Belenkiy. E-Cash. In Handbook of Financial Cryptography and Security. CRC, 2011.

[16] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from Bitcoin. In IEEE Symposium on Security and Privacy, 2014.

[17] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza. SNARKs for C: Verifying program executions succinctly and in zero knowledge. In CRYPTO, 2013.

[18] E. Ben-Sasson, A. Chiesa, M. Green, E. Tromer, and M. Virza. Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs. In IEEE Symposium on Security and Privacy, 2015.

[19] I. Bentov and R. Kumaresan. How to Use Bitcoin to Design Fair Protocols. In CRYPTO, 2014.

[20] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld. Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake. Cryptology ePrint Archive, Report 2014/452, 2014.

[21] A. Biryukov and I. Pustogarov. Bitcoin over Tor isn’t a good idea. In IEEE Symposium on Security and Privacy, 2015.

[22] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore. Sybil Resistant Mixing for Bitcoin. In WPES’14: Workshop on Privacy in the Electronic Society, 2014.

[23] J. Bonneau. Why ASICs may be good for Bitcoin. https://freedomto-tinker.com/blog/jbonneau/why-asics-may-be-good-for-bitcoin/, December 2014.

[24] J. Bonneau and P. Eckersley. Agile Tokens, 2014.

[25] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies (Extended Version). Cryptology ePrint Archive, Report 2015/261, 2015.

[26] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten. Mixcoin: Anonymity for Bitcoin with accountable mixes. In Financial Cryptography, 2014.

[27] J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Compact ecash. In EUROCRYPT, 2005.

[28] D. Chaum. Blind signatures for untraceable payments. In CRYPTO, 1982.

[29] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In CRYPTO, 1990.

[30] N. Christin. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In WWW, 2013.

[31] J. Clark and A. Essex. CommitCoin: carbon dating commitments with Bitcoin. In Financial Cryptography, 2012.

[32] M. Corallo. High-speed Bitcoin Relay Network, November 2013.

[33] N. T. Courtois. On the longest chain rule and programmed selfdestruction of crypto currencies. arXiv preprint arXiv:1405.0534, 2014.

[34] N.T.Courtois, M.Grajek ,and R.Naik. Optimizingsha256inbitcoin mining. In Cryptography and Security Systems, 2014.

[35] O. Coutu. Decentralized Mixers in Bitcoin. Bitcoin Conference, 2013.

[36] W. Dai. b-money. www.weidai.com/bmoney.txt, 1998.

[37] G. Danezis, C. Fournet, M. Kohlweiss, and B. Parno. Pinocchio Coin: building Zerocoin from a succinct pairing-based proof system. In PETShop, 2013.

[38] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In IEEE P2P, 2013.

[39] A. K. R. Dermody and O. Slama. Counterparty announcement. https: //bitcointalk.org/index.php?topic=395761.0, January 2014.

[40] J. A. D. Donet, C. P´erez-Sola, and J. Herrera-Joancomartı. The Bitcoin P2P network. In Workshop on Bitcoin Research, Jan. 2014.

[41] dree12. List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses. bitcointalk.org, August 2014.

[42] C. Dwork and M. Naor. Pricing via processing or combatting junk mail. In CRYPTO, 1992.

[43] S. Eskandari, D. Barrera, E. Stobert, and J. Clark. A ﬁrst look at the usability of bitcoin key management. Workshop on Usable Security (USEC), 2015.

[44] I. Eyal. The Miner’s Dilemma. In IEEE Symposium on Security and Privacy, 2015.

[45] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography, 2014.

[46] J. Garay, A. Kiayias, and N. Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive, Report 2014/765, 2014.

[47] L. Garber. Government Ofﬁcials Disrupt Two Major Cyberattack Systems. IEEE Computer, July 2014.

[48] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun. Is bitcoin a decentralized currency? IEEE Security & Privacy, 12(3):54–60, 2014.

[49] A. Gervais, G. O. Karame, D. Gruber, and S. Capkun. On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin clients. In ACSAC, 2015.

[50] S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, E. W. Felten, J. A. Kroll, and A. Narayanan. Securing bitcoin wallets via a new DSA/ECDSA threshold signature scheme, 2014.

[51] D. M. Goldschlag and S. G. Stubblebine. Publicly Veriﬁable Lotteries: Applications of Delaying Functions. In Financial Cryptography, 1998.

[52] R. Grinberg. Bitcoin: An Innovative Alternative Digital Currency, November 2011.

[53] M. Hearn. Dan Kaminsky’s thoughts on scalability. bitcointalk.org, 2011.

[54] M. Hearn. Merge-Avoidance: a note on privacy-enhancing techniques in the Bitcoin protocol. medium.com, 2013.

[55] M. Hearn. Rapidly-adjusted (micro)payments to a pre-determined party. bitcointalk.org, 2013.

[56] J. Herrera-Joancomart. Research and Challenges on Bitcoin Anonymity. Keynote Talk: 9th International Workshop on Data Privacy Management, 2014.

[57] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko. Botcoin: monetizing stolen cycles. In NDSS, 2014.

[58] jav. Instawallet introduces new approach to instant payment: Green address technique. bitcointalk.org, July 2011.

[59] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In Workshop on Bitcoin Research, 2014.

[60] G. O. Karame, E. Androulaki, and S. Capkun. Double-spending fast payments in Bitcoin. In ACM CCS, 2012.

[61] R. Karp, C. Schindelhauer, S. Shenker, and B. Vocking. Randomized rumor spreading. In Foundations of Computer Science, 2000.

[62] S. King. Primecoin: Cryptocurrency with prime number proof-ofwork, 2013.

[63] S. King and S. Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, August 2012.

[64] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In WEIS, 2013.

[65] P. Krugman. Bitcoin is Evil. The New York Times, Dec 2013. [66] J. Kwon. TenderMint: Consensus without Mining, August 2014.

[67] S. M. Larson, C. D. Snow, M. Shirts, et al. Folding@ Home and Genome@ Home: Using distributed computing to tackle previously intractable problems in computational biology. Technical report, arXiv preprint, 2002.

[68] A. Laszka, B. Johnson, and J. Grossklags. When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long-Term Impact of Attacks Between Mining Pools. In Workshop on Bitcoin Research, 2015.

[69] B. Laurie. An Efﬁcient Distributed Currency, 2011.

[70]B. Laurie. Decentralised currencies are probably impossible (but let’s at least make them efﬁcient), 2011.

[71]B.Laurie and R.Clayton. Proof-of-work proves not to work. In WEIS, 2004.

[72]T. B. Lee. Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%. Ars Technica, March 2013.

[73]S.D.Lerner. Even faster block-chains with the DECOR protocol. https://bitslog.wordpress.com/2014/05/02/decor/, May 2014.

[74] S. D. Lerner. The Private Automatic Miner Backbone Protocol (PAMBA), April 2014.

[75]P.Litke and J.Stewart. Cryptocurrency-stealing malware landscape. Technical report, Dell SecureWorks Counter Threat Unit, 2014.

[76] A. Loibl. Namecoin. namecoin.info, 2014.

[77] makomk. [DEAD] Coiledcoin - yet another cryptocurrency, but with OP EVAL! bitcointalk.org.

[78] J. Matonis. The Bitcoin Mining Arms Race: GHash.io and the 51% Issue, July 2014.

[79]G.Maxwell. CoinJoin: Bitcoin privacy for the real world. Bitcoin talk. org, August 2013.

[80] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In IMC, 2013.

[81] I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In IEEE Symposium on Security and Privacy, 2013.

[82] A. Miller. Feather-forks: enforcing a blacklist with sub-50% hash power. bitcointalk.org, October 2013.

[83] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz. Permacoin: Repurposing Bitcoin Work for Data Preservation. In IEEE Symposium on Security and Privacy, May 2014.

[84] A. Miller and J. J. LaViola Jr. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin, 2014.

[85] A. Miller, E. Shi, A. Kosba, and J. Katz. Nonoutsourceable Scratch Off Puzzles to Discourage Bitcoin Mining Coalitions (preprint), 2014.

[86] T. Moore and N. Christin. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In Financial Cryptography, 2013.

[87] M. M¨oser and R. B¨ohme. Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. In Workshop on Bitcoin Research, 2015.

[88] M. M¨oser, R. B¨ohme, and D. Breuker. An inquiry into money laundering tools in the Bitcoin ecosystem. In IEEE eCrime Researchers Summit (eCRS), 2013.

[89] M. M¨oser, R. B¨ohme, and D. Breuker. Towards Risk Scoring of Bitcoin Transactions. In Workshop on Bitcoin Research, 2014.

[90] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. http: //bitcoin.org/bitcoin.pdf, 2008.

[91] T. Nolan. Alt chains and atomic transfers. bitcointalk.org, May 2013.

[92] T. Okamoto and K. Ohta. Universal electronic cash. In CRYPTO, 1992.

[93] M. Okun. Agreement among unacquainted Byzantine generals. In Distributed Computing. 2005.

[94] M. Palatinus. Stratum mining protocol – asic ready. https://mining.bitcoin.cz/stratum-mining, September 2012.

[95] R. Parhonyi. Micropayment Systems. In Handbook of Financial Cryptography and Security. CRC, 2011.

[96] C. Percival and S. Josefsson. The scrypt Password-Based Key Derivation Function, 2012.

[97] A. Poelstra. Distributed Consensus from Proof of Stake is Impossible, May 2014.

[98] Quantum Mechanic. Proof of stake instead of proof of work. bitcointalk.org, July 2011.

[99] R.L.Rivest. Peppercoin micropayments. In Financial Cryptography, 2004.

[100] R. L. Rivest and A. Shamir. PayWord and MicroMint: Two simple micropayment schemes. In Security Protocols Workshop, 1997.

[101] S. Ro. A Bloomberg TV Host Gifted Bitcoin On Air And It Immediately Got Stolen. Business Insider, December 2013.

[102] M. Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems. Technical report, CoRR, 2011.

[103] M. Rosenfeld. Overview of Colored Coins, 2012.

[104] T. Rufﬁng, P. Moreno-Sanchez, and A. Kate. CoinShufﬂe: Practical decentralized coin mixing for Bitcoin. In ESORICS, 2014.

[105] T. Sander and A. Ta-Shma. Auditable, anonymous electronic cash. In CRYPTO, 1999.

[106] T. Sander, A. Ta-Shma, and M. Yung. Blind, auditable membership proofs. In Financial Cryptography, 2001.

[107] B. Schoenmakers. Security aspects of the EcashTM payment system. State of the Art in Applied Cryptography, 1998.

[108] D. Schwartz, N. Youngs, and A. Britto. The Ripple Protocol Consensus Algorithm. https://ripple.com/consensus-whitepaper/, September 2014.

[109] SEC vs Shavers. https://www.sec.gov/litigation/complaints/2013/ comp-pr2013-132.pdf, 2013.

[110] M. Sirbu and J. D. Tygar. NetBill: An internet commerce system optimized for network-delivered services. IEEE Personal Communications, 2(4):34–39, 1995.

[111] E. G. Sirer and I. Eyal. How to Disincentivize Large Bitcoin Mining Pools, June 2014.

[112] Y. Sompolinsky and A. Zohar. Accelerating bitcoin’s transaction processing fast money grows on trees. Not Chains, 2013.

[113] I. Stewart. Proof of burn. bitcoin.it, December 2012.

[114] N. Szabo. Formalizing and securing relationships on public networks. First Monday, 2(9), 1997.

[115] M. B. Taylor. Bitcoin and the age of bespoke Silicon. In CASES, 2013.

[116] J. Tim´on and M. Friedenbach. Freicoin - easy-to-use demurrage currency. <http://freico.in/>.

[117] J. Tromp. Cuckoo Cycle: a memory-hard proof-of-work system. In Workshop on Bitcoin Research, 2015.

[118] L. Valenta and B. Rowan. Blindcoin: Blinded, Accountable Mixes for Bitcoin. In Workshop on Bitcoin Research, 2015.

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

[120] M. Vasek, M. Thornton, and T. Moore. Empirical analysis of denialof-service attacks in the Bitcoin ecosystem. In Workshop on Bitcoin Research, 2014.

[121] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer. Karma: A secure economic framework for peer-to-peer resource sharing. In Workshop on Economics of Peer-to-Peer Systems, 2003.

[122] F. Voight. p2pool: Decentralized, dos-resistant, hop-proof pool. https://bitcointalk.org/index.php?topic=18313.0, June 2011.

[123] J. R. Willett. MasterCoin Complete Speciﬁcation, v1.1, 2013.

[124] wizkid057. Re: [6600Th] Eligius: 0% Fee BTC, 105% PPS NMC, No registration, CPPSRB (New Thread). bitcointalk.org, June 2014.

[125] G. Wood. Ethereum: A secure decentralized transaction ledger. http: //gavwood.com/paper.pdf, 2014.

1. 我们将会看到，可能无法删除货币功能，而且仍然有一个工作共识系统。 [↑](#footnote-ref-1)
2. 有趣的是，第一个区块包含字符串“时间03/Jan/2009，在银行第二次救助的边缘”。 [↑](#footnote-ref-2)
3. 分别可以在https://github.com/bitcoin/bitcoin/ bips，<https://bitcointalk.org/>，https://bitcoin.it/bitcoin-development@lists. sourceforge.net，irc//freenode.net/#bitcoin-dev和

   irc：//freenode.net/＃bitcoin-wizards 中找到 [↑](#footnote-ref-3)
4. 事实上，每当比特币使用SHA-256，散列函数实际上应用了两次。这可以表示为SHA-2562，但我们忽略了这个符号。 [↑](#footnote-ref-4)
5. 在块中发布之前，由于交易的可延伸性，交易的散列不是唯一的ID[6]。 [↑](#footnote-ref-5)
6. 大写的“比特币（Bitcoin）”是指整个系统，而小写的“比特币（bitcoin）”是指一个货币单位。 [↑](#footnote-ref-6)
7. 比特币的挖掘难题不是一个真正的工作证明方案，而是一个概率方案。找到一个解决方案在计算上对期望有挑战性，但有可能只是得到了运气，只需很少的工作就能找到一个解决方案。 [↑](#footnote-ref-7)
8. 特别是，这样可以防止攻击者使区块链分叉，修改分叉上的时间戳以产生较低的困难，并且使用这种较低的难度更容易地超越以前的最长的链。 [↑](#footnote-ref-8)
9. 在写者篇论文的时候，d≈68 [↑](#footnote-ref-9)
10. 这个难题稍微复杂一些，因为随机性被分割成区块链顶端的32个随机数以及在比特币交易中的任意“额外随机数”。绝大多数矿工通过选择一个随机的临时值，然后为了算出顶端的值算尽所有232个数 [↑](#footnote-ref-10)
11. 合理的检查是为了防止操控时间戳而戏剧性地改变难度。含有难以置信速度的时间戳将被网络拒绝。 [↑](#footnote-ref-11)
12. 例如：Andrychowicz等人 [5]报告需要将其复杂的多种形式的“彩票”脚本直接提交给Eligius矿池。 [↑](#footnote-ref-12)
13. 这有时被称为“诚实”挖矿，但是我们忽略了一点：不合规的策略也有可能被当作诚实的。 [↑](#footnote-ref-13)
14. 这种攻击策略被被Eyal和Sirer称为自私采矿[45]，他们是第一个分析它的人。 [↑](#footnote-ref-14)
15. 例如，CoiledCoin就是一个由比特币矿池Eligius的重大攻击而摧毁的一个山塞币。 [↑](#footnote-ref-15)
16. 对于比特币本身，最初中本聪是唯一的一位矿工，到2011年积累了超过1亿1千万比特币的资金，其中大部分还没有用完。 [↑](#footnote-ref-16)
17. 此问题在其他应用程序中也有应用，包括密码散列和基于密码的加密，目前的密码散列竞赛正试图确定新的标准。 [↑](#footnote-ref-17)
18. 另一种支付方式是使用多个不同的商户地址来避免合并[54]，但这还没有被标准化或被采用。 [↑](#footnote-ref-18)
19. 在VII-B章中的CoinJoin是一个例外，它明确使用多输入交易来增强匿名性。 [↑](#footnote-ref-19)
20. “燃烧证明”也是一个解决方法，但这是不可证实的，所以矿工也不鼓励这种行为。 [↑](#footnote-ref-20)