SoK：Bitcoin and Cryptocurrencies研究的前景和挑战

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——比特币是至今在历史上最为成功的加密数字货币。在其默默无闻地于2009年发行后的两年间，尽管只是经过粗略估计它的系统结构，比特币就已经成长到市值十亿美元左右。自此之后，越来越多识别比特币系统中隐藏的重要属性的文献不断发表，这些文献发现了系统攻击的理论，提出了有潜力的替代品，并提出了困难的未来挑战。与此同时，一个庞大而活跃的开源社区已经提出并部署了大量的修改和扩展条约。**

**我们提供了首个对于比特币和诸多相关加密数字货币或称“替代币”的系统的阐述。从中提取一个分散的知识体系，我们识别出三个可以拆分的比特币系统设计的重要组成部分。这使得我们能够更深入地分析比特币的性能和稳定性。我们为被提出的众多的修订方案绘出了设计空间，为可替代的一致机制、货币分配机制、计算问题、和关键的组织工具提供了比较和分析。我们调查了比特币中的匿名性问题，并提供了一个评估结构，用于分析各式各样的有关提高隐私性建议书。最后，我们对于如何在应用中免除对仲裁机构，也就是我们所说的中介机构的需求，提出一个全新的深刻理论。我们还鉴别了三种起中介机制的策略并进行了细致的比较。**

## Ⅰ. 为什么比特币值得研究

首先基于稻草人论证，我们讨论一下对于比特币的两种相对的观点。第一种观点认为：“比特币在实践中运作良好，但在理论上并无根据。”经常有比特币团队中的成员信奉这个哲学，他们因为专门研究安全理论的团队没有发现比特币的机理，也基于目前缺乏严密的理论基础的事实，直至今日仍然嘲笑和贬低那些进行安全理论研究的团队。

第二种观点认为，比特币的稳定依赖于一种未知的社会经济因素的组合，这种组合对模型的精确度是无可救药的，但却无法为系统的可靠性提出令人信服的论据。由于上述困难，经验丰富的安全理论学者一般会规避“比特币”这个研究课题，为保证研究工程的谨慎，所以只研究有公认的安全证明、精确的威胁模型的系统。

我们想要说明这两种过于简单化的观点都有瑕疵。首先，我们认为尽管比特币系统到目前为止在实践中取得了令人惊讶的良好结果，但是理论研究在识别其运作良好的原因中扮演着重要的角色，并能帮助我们超越以往对于支出比特币最初系统设定的通俗理论的盲目接受。再者，理论的研究对于理解比特币系统能否在现实条件变化下依旧会运作良好起着关键的作用。外部的政治与经济因素正在逐步构建，交易量的衡量和矿工的货币奖励的本质会遵循系统的设计而变化，因此比特币系统必须做出相应改变。仅仅由于比特币系统在2009-2014年运作良好，是不足以推断它会像这样持续良好运作下去。我们对其没有足够的认识去自信地推断比特币将会继续在未来运作良好，而这个推断，也是一个需要计算机科学理论洞察力的关键性研究挑战。

其次，我们认同比特币通过提供虚拟的货币系统填补了一个重要的市场，这种虚拟的货币系统不需要任何值得信赖的政党机关或预设的参与者身份。在这些约束条件下，分布式系统中普遍存在的协商一致问题是不可能发生的[7], [93]，没有更进一步的假设如比特币的前提是合理（贪心）的行为，可以被模仿，奖励可以被均衡，来确保一致性算法的安全运作。尽管这些限制条件从哲学上和技术上对实践很重要，但比特币在它的模型中保证一致性的办法仍然极其令人吃惊，并且有根本性的贡献。比特币核心的共识协议对于很多的除了货币1的计算机安全问题都有着深远的影响，其中不只在货币领域，还有分布式命名、时间戳、承诺、一代用户的随机性、和一些经济问题如智能合约、去中心化市场、发货簿和分布式自治合同等。总而言之，尽管比特币系统并不好模仿，但是由于它很有可能提供很多极其复杂但是关键问题的实践性解决策略，仍然值得进行大量的研究。

明白这个分歧之后，我们开始综合比特币在运行和发展六年间的集体智慧，同时也从其衍生的加密数字货币得到了一些结论。我们不仅想强调出现了很多重要创新的领域，范围从新型支付条约到用户友好型关键管理技术，还想强调的对于比特币和未来的加密型货币的重要的开放性研究的挑战。

## Ⅱ. 比特币的概述

### A．文字化历史

我们向有兴趣的读者推荐现存的有关加密型币的第一次浪潮的调查[15],[95]。总而言之，加密货币要追溯到Chaum在1983年的对于“无迹可寻的支付”的假说[28]，这种系统基于银行以符号形式发行的虚拟货币。确实

1正如我们所见，它可能不可能移除货币功能，但仍有一个工作共识系统。

存在的货币在商人和使用者之间转移，并在银行确认未赎回后才可以被赎回。

但虚拟签名却可以避免以银行连接用户和商人，对货币也可提供类似的非关联性。

贯穿二十世纪九十年代，很多比特币的变式和拓展被提出。其中的重要贡献包括：在网上购物时无需借助银行[29]、允许货币被分割成诸多小的整体[92]、提高效率[27]。很多刚刚起步的公司包括DigiCash[107]和Peppercoin[99]都企图实施电子货币协议但最终都在市场中失败了。在加密货币的第一次浪潮中，没有任何一个计划有至关重要的进度。

PoW机制作为比特币的一个重要的基础构建，是在二十世纪九十年代初被提出的，但最初是为了在邮件刷屏中战斗[42]，尽管它最终并没有在此用途上广泛展开[71]。很多其他的应用也紧随其后，包括公平彩票制的提出[51]，为小额交易铸币[100]，防止网络中各种匿名的阻断式服务攻击[10]，后者，Hashcash，是用电子加密货币的另一种替代选项（例如NetBill[110]和Karma[121]）。PoW机制也在分布式对等一致协定中被用于察觉同级节点[7]，这与其在比特币一致性中的作用类似。

比特币的另一个重要组成部分是公共总账，它使得双支付问题的察觉成为可能。在二十世纪九十年代后期，在可审计的电子货币领域中[105], [106]，尽管原本发布一整套货币的概念由于缺乏可行性而不予考虑（作为替代只发布了一个Merkle根），银行依旧维持着一份公众的数据库，用于鉴别双支付并确保货币的有效性。B-money在1998年被提出[36]，成为第一个所有交易完全公开发布（尽管使用化名）的系统。被发布在密码朋克邮寄清单上之后，B-money收获了少量学术研究人士的关注。

智能合约在二十世纪九十年代初期被提出[114]，在它的作用下，政党可以选择正式地指定一个加密型货币的强制实行合约，并将其作为比特币脚本处理容量的延伸。

在2008年比特币问世，中本聪以此假名在密码朋克邮寄清单上发表了比特币白皮书[90]，很快就有了最初用户的原始代码。比特币的创世区块大概在2009年1月3日2被开采出来。比特币的首次交易是在2010年3月，一位用户以1万比特币的价格订购了一份披萨。在那之后，越来越多的商人和服用都采用了比特币作为支付手段，而比特币的价格也水涨船高，在2013年年末甚至达到了1比特币相当于大概1200美元的最高价格。

比特币的历史也被其相关的犯罪所粉饰，Silk Road[30]作为一个热门的黑市网站从2001年2月一直运作到2013年10月被FBI关停。僵尸网络也发现在比特币开矿是一种追加的收入来源[57]。近期一起注明的美国联邦法庭案件涉及到关于比特币的庞氏骗局[109]。在2014年，一个叫做敲诈者的病毒公司通过加密文件，然后要求赎回比特币来获得密钥的犯罪行为欺诈了上百万美元[47]。很多用户还发现他们的比特币由于被偷[41]而丢失或突然减少[86]。

### B. 技术概述

我们将展示比特币的三个重要的技术组成部分：交易（包括小额交易）、一致性协定、公开通讯网络。比特币是极度复杂的——而在这篇论文中，我们的目标是以足够的技术深度来展示比特币系统，并在这篇论文的后面章节中评价以往的文献。特别的是，我们从这三种方面来展开的结构可以更加深入清晰地分开叙述和探讨它们的概念，毕竟这些概念是独立变化的。

**比特币系统的信息来源。**由于没有一

2著名的ﬁ第一块包含字符串“03 / 1 / 2009财政大臣濒临银行第二轮救助的边缘。”

个官方的权威的说明书，我们很难去定义比特币。最原始的比特币白皮书为比特币的设计哲学提供了一个不错的概念[90]，但是很多重要的技术细

节要不被忽视，要不就太过时了。我们将把比特币的实施作为一个事实上的说明，还会参考分散在一系列BIPs、论坛的帖子、维基百科文献、开发者邮件清单和粗略的IRC讨论中的知识。3把这些来源系统化地分类得到精确的技术介绍，并提出我们认为相当重要的、出于独立设计的系统组件。

1）交易脚本：一系列称为交易的信息代表了比特币系统中的区块。在各种方案中，交易信息是用户之间转移资金的首要发布信息。需要强调的概念是大量且不断增长的交易记录是比特币区块的唯一表示。对于用户，现在还没有一个高级的概念来描述，账户平衡和账号这些概念只需要能够在公开的交易记录中被追溯到即可。

**交易格式。**一个交易信息包含一个输出的数组和一个投入的数组。完整的交易信息会被SHA-2564分散排列，接着这个分散排列最终5作为其全球独一无二的交易ID。交易数据用一种特别的二进制格式代表。这是一种早期说明“比特币是事实上的说明书”的重要例子。

每次的产出都包括一个整体的价值，这个价值代表了比特币货币的数量。这种价值的精度限制了货币集体被细分的程度，最小而不可再分的货币集合被称为1中本聪。按照惯例，10^8中本聪被认为是货币的初级集合，也

被称为1比特币6，表示为、BTC 或

3可以分别在：t: 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找到

4事实上，当比特币使用SHA-256散列函数的应用，实际上是两次。这可能是表示sha-2562，但我们忽略了这个符号。

5在一块出版之前，交易的散列ID并不是唯一因交易延展性[ 6 ]。

XBT。

每次的产出还包括一段小的编码片段（以一种特殊的脚本语言表示），这段编码片段也被称为“scriptPubKey”，它意味着交易记录可以被赎回，并可以作为下一次交易的投入。

**交易脚本。**一般来说，scriptPubKey指定了一个ECDSA的分散数据和署名生效程序。因此，这也被称为“pay-to-pub-key-hash”交易，整个赎回交易也必须被特定分散的密钥标记。绝大多数的比特币交易都是“pay-to-pub-key-hash”交易，所以尽管其他种类的交易也可以实现，这种交易还是被描述为比特币系统的唯一交易类型。脚本语言事实上是一种非图灵完整性的堆叠语言，它只有不到200条称为操作码的指令。它们包括加密货币运作的支持，例如哈希数据和核实的签名。正如交易格式一样，脚本语言只能由比特币中的说明书来特定指明。

交易输入涉及到之前的交易记录的交易哈希值和产出数组的指数。它们当然也包含一小段用于赎回被称为scriptSig的交易产出的编码。为了成功地赎回之前的交易，scriptSig和scriptPubKey必须同时以同样的堆叠方式相继成功执行。对于“pay-to-pub-key-hash”交易来说，scriptSig仅仅只是一个有着正确哈希值的公共密钥和署名而已。

**价值守恒。**除了后面的交易投入要与之前的交易产出对应并且两个脚本要成功运作之外，只有交易数据满足所有交易产出小于等于交易投入的基本的约束，这个交易数据才是有效的。我们之后会在第Ⅱ章B2节讨论交易中用来创造新的资金集合的金矿的概念。

**从交易记录到所有权。**这种交易格

式本身就蕴含了很多有趣的性质。对

6当资本化“比特币”是指整个系统时，小写“比特币”是指一种货币单位。

于比特币的所有者并没有说明固有的概念。所有权仅仅意味着得知一个可以做标记并赎回比特币的私人密钥。而在“pay-to-pub-key-hash”交易中被指明的公共哈希密钥，可以以匿名身份在系统中成功运用，并以地址的名义被涉及。

可论证的是，比特币的交易格式中有微小但是很深入的创新。但是用脚本语言来指明赎回标准、用交易来指明整个系统区块的实现并不是一个显而易见的选择，因为在之前的加密货币系统中，这两者在后期的设计中基本上都合乎标准。一些提议延伸了比特币交易的语义学意义（通常是提升了脚本语言），但都不包括比特币的其他的组成成分。

2）共识机制和挖矿：在一个以交易为基础的货币系统中，如果交易时用户之间直接转移资产，安全性无法保证。尽管签名可以通过以先前交易的有效接收者作为参考信息限制其后续的交易，但是这个系统本身并不能限制一个人赎回投入两次并分别转给两个人，这两次交易分别都是有效的。比特币采取了一个简单的办法来解决上述双支付问题：所有的交易都必须在公开且永恒的交易日志上发表，任一单独的交易产出都只能在后续交易中赎回。因此现在若想核实以此交易的真实性，不仅得核实交易脚本，还需确保它是完整发布在交易日志上的。在比特币系统中，交易日志被说明为一系列交易区块，每一个交易区块都需要前一区块的哈希数，在这个区块中检入其特定前情。这些区块相连就构成了区块链。

值得一提的是这种设计依然需要对区块链达成全球共识。如果不同的用户看到的是相异的区块链，他们就容易受到双支付攻击。一种解决方案是设置一个公允的权威机构，让它来收集交易信息并记录在已知区块链中。但是这种办法也有缺点，因为这个权威机构可能不愿意发布一些特定的交易信息（高效地冻结某些用户的资产），可能会完全在线下运行，可能由于双支付问题引起分叉。

**中本共识机制。**比特币没有建立以上机制，反而建立了一个去中心化共识机制，这种匿名化的协定也被称为中本共识机制。可以说，这种机制是比特币机制的核心创新，而且也许是其成功的最关键因素。任何节点都可以通过收集一系列有效的后续交易信息并加入区块链中。最核心的组成部分是使用具有一定难度的计算难题（通常是被给予一个要求较小误差的工作量证明问题7）来决定哪个节点的区块可以作为区块链的下一区块。

选择下一区块的方法非常简单：第一个宣布了有效的正确计算答案的区块。当其他节点得知该区块链的记账权已经有归属后，便会转而为成为下一区块而努力。如果公布的区块包含了错误的交易数据或是有缺陷的话，其他节点就不会接受该结果并继续为了获得该区块的记账权而努力，直到他们得到了获得新区块的有效答案。不论何时，公认的主区块链都是最长的区块链。特别的是，主区块链实际上也只是有着最多区块的链，但是由于挖矿的难度在区块的不同分叉上并不相同，所以主链必然是计算工作量最大的一条链。8

在此情形下，同时有两个节点几乎在同时得出了有效的答案也是有可能的（依赖于网络工作的潜在因素），这就会导致产生两个相同长度的分支。之后，矿工们可以任意选择一个分支。由于计算问题的随机性，其中一条支链会比另一条支链延伸地更长，在那

时所有的矿工都应选择那条长链。

7比特币的采矿难题不是一个真正的工作计划证明，而是一个概率的证明。找到一个解决方案是计算具有挑战性的期望，但它是可能得到幸运和用很少的工作找到解决方案。

8明确的说，这可以防止攻击者从分叉的区块链修改时间戳在分叉产生较轻困难，而且用低难度的更容易超越以前的长链。

虽然比特币的最初说明中只提供一条非正式的论证说明最终的共识将会浮现[ 90 ]，后续的工作证明，假设一个有效和及时的广播公共频道和控制大部分的计算能力的矿工遵循协议。条约将具有鲁棒性，并且网络会达成最终共识[46]，[84]。我们将在第Ⅲ章中详细讨论。

**区块确认。**这种共识机制的自然特性意味着：用户必须要等待新区块形成才能确认这笔交易被永久地记录在区块链中，如此一来交易才是有效的。在分叉时，当所有矿工都汇聚在一条链时，另一条链最终会被废弃。尽管这两条链包含的主要是同样的交易数据，但是如果有矛盾的交易信息被包含于分支的竞争当中，且有可能被包含于显然较长的那条链，那么由于短链优于长链，长链会被废除。更可怕的是，这种情形很有可能会引发双支付问题[12]，[60]。

所以理论上来说，用户永远都无法确定交易是否在分支中被移除[13]，[70]。但是，如果绝大部分的矿工都遵从默认条约，且不断有后续区块产生时，用户可以推测该交易在最终长链上的可能性以指数形式增长（解释于第Ⅲ章第A节）。实际上，大多数的比特币用户一般需要6个确定的后续区块就可以判断该交易被成功发表了。这6个区块的选择是任意的，它起源于用户，但是与分支的可能性分析没有任何关系。

分支也可以用一种专门的方式去规避，包含了硬编码的区块链前缀（检查点）和默认的在任何有效区块链中都需要的比特币用户。Laurie[70]指出这些前缀证明了比特币不是一种真正的去中心化的公式条约，因为它们是以一种中心化的方式选择。

**以物质激励正确的行为。**条约的一个关键组成部分是：任何一个用户，只要在发现在某区块中可以插入金矿交易数据，都可以通过挖矿获得一定金额的货币并转移到其指定的地址。因为这些用户在不断工作（实际上是在竞争）去解决计算难题以期获得资金奖励，所以他们也被称为矿工。由于失效的区块链最终会被网络撤销，于是矿工的计算成果就不会在最终的总区块链上出现，这种资金奖励不断地激励矿工只在有效的区块计算。特别的，从矿工的视角来看，“有效”的区块就是他们相信大多数的矿工都会选择工作的区块，而不是任何说明中的有效性。（那些说明都属于比特币说明中的观点）。

因为这种共识算法依赖于对矿工的资金奖励，所以很容易在那些没有明确可转让财产概念的系统中实施。在比特币系统中，矿工们最初受到的都是新的货币，而且并没有其他的创造货币的机制。这种奖励机制不是必须的，但是共识条约确实需要给矿工发布一些资金奖励，如若不然，矿工们就没有寻找有效区块和解决计算难题的动力了。

**挖矿细节。**这种计算问题需要各节点为SHA-256问题寻找一个局部的原相，这种SHA-256问题是一种哈希密码结构。特别的是，提出这个问题是为了寻找一个新的区块（包括一系列交易数据，前一区块的哈希值，时间戳，还有一个随机数值），这个区块的SHA-256哈希值必须小于目标值。这个问题常常被描述为寻找一个以d连贯的零位。9标准策略是不断尝试随机值10直到找到解决答案（尽管这可能不是唯一的策略[34]）这个问题的随机性是相当重要的，因为在一个非随机性的问题中（真正的工作量证明问题），拥有最多算力的节点应该会第一个获得每个区块。但是在随机性问题中，

每个矿工与其算力成比例的可能找到9在写这篇文章时d≈68

10问题更复杂的是，随机分成块中的头一个32位的随机数和任意一个“额外的临时“在Coinbase交易。大多数矿工进行选择一个随机的Coinbase杜撰然后用尽所有232值为头数。

下一个区块。

通过灵活调整问题的难度，可以保证新区块的生成速率平均为10分钟一个。为了维持这种速度，每创建2016个比特币甚至需要系统每两周都要参考那2016个区块的时间戳来调整问题的难度。

**挖矿奖金和劳务费。**新区块的奖励是由一个调整方案来决定的。最初，每个新区块会创造50B。这50B在之后会被减半到25B，而且每过四年会周期性地不断减半，直到大概2140年之后就再也不会产生新的比特币了。为了使这个不断衰减的货币制造系统继续运转，矿工不仅可以从挖矿奖励中得到报酬，也可以从当前区块的所有交易的投入、产出中索要一定的价值。对于用户来说，在一个投入大于产出价值的区块中，实际上是有一部分作为劳务费付给了矿工。11

至今为止，交易劳务费主要用于防止线上小额交易（被称为penny ﬂooding）的滥用，而且劳务费不会多于总挖矿收益的1-2%[87]。劳务费最初由用户违约形成的[87]，另外还有一些用户选择支付更高额的劳务费而使得他们的交易信息被更快发布。

**金矿。**实际上，为了降低在挖矿中收益的波动，矿工经常在挖矿中互相合作[102]，与同组的矿工一起分享挖矿奖励。采矿池通常由管理人员管理, 他们收取少量费用, 从所有参与成员发现的有效区块中收集采矿奖励, 并按金矿的工作量分配资金给成员。参与的矿工通过给以大量0开头的哈希值但无有效比特币的临近区块发送股份证明自己的工作量，以期交换得到一些收益，用以支付管理者的管理费。

尽管在最初的比特币说明书中并没有描述，是未预料到的产物，但是自从2013年开始大部分的算力都在金

矿中发挥作用。一部分的准则用来为11检查是为了防止操纵时间戳从而大大改变了不同的困难值。难以置信的时间戳块将被网络拒绝。

矿工们分割收益，这么做是为了在对新来者友好的情况下鼓励劳动，并最小化收益波动[102]。还有很多等级条约是为矿工与管理者及不同金矿之间的低延迟沟通而设定的[94]，[32]，[74]。尽管最热门的金矿都是中心化运作的，但是事实上依然有使用对等条约来运作的金矿[122]。

3）对等交流网络：比特币系统的最后一个中心组成部分就是它的交流网络。需要强调的是，它是去中心化的、对等传播网络，最初被用于宣布新的交易信息和新区块的产生。通常而言，这是三个重要组件中最缺乏创新性的，但是几乎没有替代数字货币做出实质性改变。

**对共识的冲击。**网络的性能和稳定性对共识协议有重要影响, 有两个重要原因。首先, 在其他节点之间发现一个新区块的延迟会提高产生分叉的可能性。由于畏惧产生分叉，所以在最初的设计中将产生区块的时间定为10分钟。其次, 如果一个恶意的矿工控制了相当一部分的网络，可能会试图公布有利于他自己区块的广播, 以增加他们在分叉中获胜的几率，通过这种途径来提高自己的挖矿奖励。同样, 任何能够审查网络的团体都有选择阻止某些传输和冻结资产的能力。因此, 对于比特币来说, 有一个去中心化并符合整体设计的广播网络是很重要的,它同时需要达到低滞后以及没有可能对消息进行审查或延迟。

**网络拓扑学及开发。**任何节点都能通过连接任意一个其他节点加入网络。根据系统默认，如果每一节点尝试建立8个对外连接就会差不多接收125个外对内的连接。那些网络地址转换的节点是不可以接受外对内的连接的，例如移动用户。加入网络的用户最初需要找到某种办法来联系上其他用户。比特币通过使用专用的姓名地址目录服务器或称为“种子节点”来达成这个目的，种子节点用硬编码编码相关用户的身份。因此，每一个节点都能保证维持一个了解的用户地址。

用户同样还使用以下两种机制在彼此之间传递信息：首先，当一个节点建立一个新的输出连接时，它会触发一连串的中继信息包含它的连接信息;其次，接收到的连接上，在已知地址列表中可以看到大量的信息。该机制建立了一个良好连接的随机网络，具有较低的低通径，适用于通过扩散快速传播信息[38]，[61]。

**沟通条约。**新的区块和未决交易洪水一般向整个网络广播。当它们听到新块的哈希值和未决交易时，节点将发送消息给所有的对等节点。如果它们还没有看到它们(通过GETDATA消息) ，对等点可以通过请求区块或事务的全部内容来响应。由于默认的节点只能更新数据一次，这可以防止无限传播；只有接替交易的信息和区块是有效的；在临时分叉中只有他们得知的第一个接替区块是有效的；也不会发布与他们已经发布的交易信息有矛盾的交易信息。这些限制是最有效的对网络信息设计的执行——固执的节点可能会传播无效且矛盾的数据，这需要所有节点都独立验证他们收到的所有信息。

**传播政策。**默认的是，比特币节点只能传播比一般交易生效规则更严格的规则批准的交易信息和区块。目的是防止各种服务器攻击——一种对经典鲁棒性的应用。鲁棒性是指：不确信你所传递的所有信息，不拘泥于你接受的东西。例如，默认节点只能传递包括从有限标准交易类型列表里的脚本交易信息。这种政策的说明是：这个系统的用户希望被包含在区块链中的非标准交易类型的交易不能使用比特币网络，但是需要直接与适合的矿工取得联络。12另一个例子是出于防

范penny-ﬂooding的目的，默认节点每12例如，Andrychowicz等人[ 5 ]报告说需要提交复杂的多方彩票脚本直接向艾里九采矿池。

分钟应该拒绝传播几千个低于0.001B的交易信息。

## Ⅲ.比特币系统的稳定性

比特币系统的稳定性已经被一些模糊而且还互相矛盾的方式定义过了，但是它大致上被认为是意味着在系统不断成长并不断有参与者尝试新型攻击的情况下，维持一个促进功能性货币运转的系统。我们会对比特币的每一个组件考虑稳定性情况。尽管稳定性结果在很强的假设下出现，比特币系统到底在哪种情况下保持稳定依然是一个公开问题。

### A．交易有效制度的稳定性

比特币系统中，关于交易有效制度的一致性是如何达成的目前还未被充分探究清楚。基线哲学是指被中本聪定义好了的制度，我们也称为正规主义。这已经调解了对于一些特定问题的矛盾。例如在最初的OP\_CHECKMULTISIG操作码中有一个良性漏洞，最终作为正规被保留了下来。

但是正规化不能完全解释最近的比特币系统了，因为一些改变成功地使系统增加了新特性（例如支付脚本哈希值[2]）。为了适应这些漏洞，一些规则也被修改了，其中最著名的例子发生在2013年3月删除一个限制有效区块大小的漏洞时。这造成了严重后果，为运用补丁的用户拒绝了较大的区块，所以产生了一个分叉。为了解决这个问题，已经更新的用户只能放弃那个已有24个区块的分叉并暂时停止工作。那个长达两个月的空窗期就是为了让老用户更新数据[1]。但是最后，漏洞成功被修理，运用补丁的用户最终被排除了，尽管可以说实现了正规化规则。

对于比特币自身来说，没有专门为更新交易有效规制规定进程。在矿工之间没有达成一致，任何变化都会永久地给系统留下分叉，因为不同人群对于主链的解释是基于他们认为的权威，而不是基于该链与其它链之间长度比较。在这时，“比特币”到底是哪种版本的解释就无法分清了。因此，尽管人们普遍认为比特币是一个去中心化的系统，但改变规则(或消除歧义)的必要性意味着内在地需要某种程度的治理，以保持现实世界中关于哪一个区块链被认为是比特币的共识[48]，[64]。

当前事实上的治理是被比特币中维持系统运行的核心开发者提供的。比特币基金会提供核心开发者的组织结构，通过捐款筹集少量资金，以支持开发团队。与其它早期的因特网协议一样，比特币没有做出正式的进程来代替粗略协商的办法来达到一致性。

### B．共识条款的稳定性

通过假设交易有效性规则的共识，人们已经作出了各种尝试来描述区块链稳定性所必须的共识协议的性质。我们系统地把由各种分析提出的特性分为五个基本的稳定性[46], [64], [84], [90]。注意不同的作者有着不同的分类和迥异的名字，我们这里只是不太正式地总结一下。

* **最终共识。**所有依附的节点都同意“什么是成为最终优秀区块链的的条件”作为前提。我们不能要求在任何时候最长的节点都是最终有效链的条件，因为这条链可能会因为临时分叉而被丢弃（或是变为“陈旧的”）。
* **指数收敛**。产生深分叉的几率为O(2−n)。这给予客户很高的信任“k-conrmations”规则将确保他们的事务被永久地包含在主链中。
* **活跃性**。新的区块会不断被加入，在一小段时间内有效的交易信息及适当的劳务费会进入区块链中。
* **准确性。**在最长主链中的区块只包含有效的交易信息。
* **公平性。**按照期望，一个算力比例为α的矿工将会获得比例为α的金矿（如果他选择的都是有效区块的话）。

如果这些性质同时具备的话，我们可以认为系统是稳定的，但是现在我们还不是很清楚是否必须要具备所有条件。货币的使用者或许会对公平性漠不关心，但是如果不存在公平性，许多用户会停止参与，这可能会威胁到其他稳定特性。

活跃性也许是最难定义的特性，目前来说也没有出现一个官方定义。显然，我们希望那些愿意付款的人有使用网络的能力，但是不清楚交易费用和需要时间的要求是否合理。严格的活跃性也暗示了一个反审查特性，这种性质对于某些人来说是不需要的，但是另一些人认为这是比特币的核心特性。

令人惊讶的是，对于一个运作中的货币来说实际上是不需要正确性的，因为参与者可以简单地忽略最长链中的无效交易信息。但是正确性确保了SPV用户的一个执行优势，能够只使工作量证明生效，而使交易信息无效（详见章节IV-A）。

**动机相容性和博弈论。**中本聪最初认为只要所有的用户都跟从自身的经济动机，比特币机制就会保持稳定[90]，这就是动机相容性。动机相容性从未在一个比特币或是加密货币文章中被正式定义；它作为一个术语的流行可能源于其直观的吸引力和营销价值。我们可以考虑顺从13的矿工的策略就是跟从默认挖矿规则工作（参照章节II-B2）。在博弈论的术语中，如果

可以证明普遍遵循是一个纳什均衡，

13这是有时被称为“诚实”的挖掘但我们避开这不符合要求的策略也可以合理地被认为是诚实的。

那么就意味着比特币的动机相容性实现，因为没有任何一个矿工有动机去单方面改变战略。这就暗示了弱稳定性的概念，如果存在其他平衡点，而普遍服从就不是唯一的平衡了。另一方面，奉行不顺从策略的矿工多于顺从的，我们就必须要问它造成的策略一致性能不能导致共识条约的一致性。

1）比特币计价工具的稳定性：我们讨论对于比特币稳定性的已知结果，假设矿工的目标仅仅是获取比特币。

仅仅是多数服从不能保证公平性。一个有趣的不符合标准的采矿策略是临时块扣留[11], [45], [46]14，在这个操作中，矿工在最初找到区块后将其保密。如果矿工发现在该区块后有两个区块，之后就连上了主链，那么他就可以独自有效率地开矿，直到网络提示已经追到了前一个区块之内，这时这个扣留的区块就可以被发布了。因为这个矿工至少掌握了大于1/3比例的算力，这一战略控制顺从战略，是因为当雇用顺从的矿工时，它会带来更高的预期采矿报酬份额。由于不知道矿工如何选择之间几乎同时宣布的区块，所以这对更低的算力水平的攻击者也很有利。一个拥有较高网络位置的攻击者也许会比对手更快公布他们扣留的区块，所以这证明稳定性本质上依赖于对沟通网络的假设。

尽管这些结果展示了对于很多的算力分配情况而言，普遍遵循不是一个纳什平衡，没有证据表明一个自私攻击的发生，而且鉴于有暂时的区块扣留策略我们还不知道会出现什么样的平衡。如果暂时性扣留发生，就是减弱系统的公平性。

**多数服从在信息公开的情况下是一个平衡。**Kroll等 [64]分析了一个简化的当所有矿工都能获得关于以发掘区块的所有信息（防止扣留）的模型。

在这个模型中，普遍遵从是一个纳什14这种攻击策略叫做自私挖掘是由Eyal和Sirer [ 45 ]第一个分析出来的。

平衡（尽管不是唯一独特的），这也说明比特币具有（较弱的）稳定性。

**多数服从暗示了指数收敛性、一致性和活跃性。**可以证明的是，随着大多数矿工的顺从，一条最长(正确)的链条将迅速出现。最初的比特币文献[90]制作了一个模型，其中有一个恶意的矿工通过“比产生真实链速度更快地产生一个替代链”来扭转交易信息。由于二项式几率随机游动最后说明那个矿工子最终会在这场比赛中输给网络中的其他节点。Miller 、LaViola [84] 和 Garay等[46]提供了更多细节的官方证据：如果大多数矿工遵循顺从策略而且通信延迟相较于发现一块新区块的实践很小，矿工们最终会认同那个不断增长的交易历史前缀而不理会非顺从矿工的策略。这足以证明除了公平性意外的所有性质（由于可能有潜在扣留），其中所指的大多数的确切数量收网络和其他条件的轻微影响。

**有了多数矿工，就无法保证系统稳定。**众所周知，一个控制着大部分算力的非顺从矿工可能会通过收集所有的采矿报酬来破坏公平，仅仅是忽略被其他人开发的区块并不断开发自己的链，而他自己的链有可能会成为主链。多数矿工能够通过删减特定交易，拒绝将其加入链中，或当它们出现在链中就制造分叉来降低活跃性。最终，大多数的矿工会通过在区块链中产生任意长分叉，降低指数收敛性，最终影响一致性，并潜在地双支付和逆转交易信息来获得利益。所有这些策略会导致名义上的利润，但是因为这些行为是可监测的，它们不会是一个矿工的长期利益来源。我们将在下一节中继续讨论这个问题。

**如果矿工可以共谋，稳定性也无法保证。**即使在没有多数矿工的情况下，较小的矿工也有可能共谋组建一个控制多数采矿权的卡特尔，并仿效任意对于多数矿工有效的战略。这个卡特尔内部是否具有稳定性、成员是否会因诱惑而背叛、外部的矿工是否可以通过提供更优惠的条件成立一个替代的卡特尔来打破它都还是未知的。矿池可能是一个技术上的卡特尔信息机制；目前还没有对于矿工对金矿的选择和在金矿之间迁移的研究。此外，对于矿工是否且怎样通过附带支付激励其他矿工加入卡特尔还没有严谨的分析。

**当挖矿奖励减少时，难以保证稳定性。**所有的结果都用到一个简化模型，其中的每个区块都有一个固定的奖励费用。计划中矿工从挖矿奖励和交易劳务费中得到的收入否定了这个假设，并且需要更复杂的模型来说明问题，这个模型需要考虑对于交易费用的分配。据我们所知，对于没有挖矿奖励或中间状态下稳定性会受到什么程度影响的官方分析，因为交易劳务费已经变成不可忽视的的收入来源**。**

2）部计价的工具的稳定性：在比特币计价工具的模型的结果中，没有提供任何令人信服的证据证明比特币实践上的稳定性（更不用说保证其今后的持续稳定），这是因为缺少被观察到的攻击，尽管大型金矿存在潜在位置可以为非顺从行为提供利益。事实上，矿工们并不纯粹是对获得名义上的比特币感兴趣，还对获得实际上的货币感兴趣。要把这个做成模型需要为矿工开发一个实用函数，它不仅包括他们赚多少比特币，还有将他们的比特币转换为现实世界的价值或其他货币的效率。矿商的策略可能会影响他们将比特币计价的财富转化为现实世界价值的能力，原因有三：

**流动性限制。**目前，以比特币兑换外币的交易的流动性通常较低。因此，攻击者可以获得大量的比特币，但是不能将它们全部转换成外币，或者只能以极小的交换速率进行转换。

**汇率有被攻击的危险。**一些非顺从的策略，特别是那些以明显方式影响稳定的策略，可能会破坏公众对比特币的信任，从而在短期内削弱对比特币的需求。实际上，在系统技术故障的情况下，已经证明交换速率明显下降[72]。能够快速赚到很多比特币的策略一旦被发现就很可能导致汇率崩溃，因此很难在汇率改变之前兑现，特别是在流动性限制下。

**在比特币计价下挖矿奖励的长期利益。**大多数大型矿工对维持比特币汇率有额外的兴趣，因为他们的重要资本固定在非流动性的采矿硬件上，如果汇率下跌，这些硬件就会失去价值。如果矿工期待用最低限度的成本长期维持他们的采矿权份额（如果他们的大部分运作成本是提前支付用来购买设备的），那么，他们可能会不选择那些赚取更多比特币，但却减少他们未来预期采矿奖励价值的策略。请注意，这是一个限制因素，即使矿工可能会在公众发觉之前迅速地将非法得到的比特币兑现，只要没有有效的市场，矿工就可以出售预期的未来采矿权。

中本聪强调一种看法[90]来降低大多数矿工攻击的可能性，他认为他们这样会永久地破坏系统（并改变汇率），而按规律运行（遵循顺从策略）在长远来看是最合算的。事实上，2014年7月的很长时间在GHash.IO金矿中的算力超过50%的网络算力，最后公开承诺在未来限制他们的算力，以避免损害系统中的信任。

不幸的是，汇率很难以可处理博弈论模型描述，因为汇率本质上取决于人的判断和市场信任。对汇率的影响和建立更正式的实际效用函数模型是一个不可忽视的问题。

3）除了挖矿收入以外的动机的稳定性：至少有两种被分析出的策略，对于其效用对于并不纯粹从采矿奖励获利的矿工来说可能是有利的。

**金手指攻击。**如果大多数矿工的目标是明确地破坏比特币的稳定性，从而破坏比特币作为一种货币的效用是很容易做到的。Kroll等[64]命名并公布了一种叫金手指攻击的模型。例如，一个希望损害比特币以避免与本国货币竞争的国家，或者一个投资于与比特币竞争的货币的个人可能会试图进行这种攻击。可以说，这些攻击已经通过杀害阿尔特钱币婴儿观察到了，比特币矿工成功地对低采矿能力的新货币进行了深分叉攻击。可以说，这些攻击已经通过溺杀替代数字货币被观察到了，对于新的有竞争力的货币的深分叉攻击已经成功上演，且只运用了很少的算力。15如果一个在未来成熟的市场出现，矿工可以在比特币的汇率上做空头交易，那么金手指类型的攻击可能可以直接获利。

**羽毛分叉**。Miller [82]提出了一个羽毛分叉策略，一个矿工试图审查交易信息黑名单，并承诺如果在块链中包含一个列入黑名单的事务，则攻击者将通过忽略包含目标交易的区块和试图对区块链进行分叉进行反击。攻击者的分叉将不断延续，最终要么速度超过主要分支并获胜，要么落后于主链，此时攻击者会公布目标交易。掌握算力小于50%的攻击者，按照预期会损失一定金钱，但成功地阻止了一宗被列入黑名单的交易，且其概率为正。

然而，如果攻击者可以令人信服地表明他们对报复分叉严重，其他矿工将动机回避目标交易也会期望如果攻击者报复。因此，攻击者可能能够执行他们的黑名单没有实际成本只要所有其他矿工相信攻击者将如果测试执行昂贵的羽毛分叉的报复。

### C．矿池稳定性

采矿池依靠参与者提交有效的块，当他们发现容易被参与者提交部分股15例如，altcoin coiledcoin altcoin被一个比特币矿池Eligius的攻击摧毁 [ 77 ]。

份换取补偿但保留有效块下池的收益。虽然这种攻击闻名已久，似乎自毁作为参与者扣块除了其他联盟成员降低自己的收入。然而，它已被证明，[ 33 ]，大商（或池）可以不使用它的一些采矿权来渗透另一池提交偏股但保留有效块来获益。这个的好处是用来渗透的容量不会持续的使挖矿问题的难度增长（由于没有公布区块）但仍可获益。这种策略有利于大矿工或池的整个范围内的挖掘能力的攻击者，在渗透池中。

Eyal[44]提供了对该攻击的扩展处理，并显示在任意两个池之间，结果游戏是一个迭代的囚徒困境，两个池的纳什均衡攻击，但不攻击的帕累托平衡。这种攻击可以在大规模的情况下进行统计，在2014年6月对Eligius pool进行了至少一次的野外调查[124]。然而，聪明的攻击者可以使用许多参与者的地址来轻松地混淆攻击。提出了进一步的对策，但没有认真研究或部署。作为一个不断重复的囚徒困境，有可能存在的资金池将避免通过渠道外通信和报复的威胁相互攻击。

### D．点对点层的稳定性

几乎所有对比特币的分析都假定点对点层的功能是指定的，一般来说，大多数参与者将在合理的时间范围内学习几乎所有可用的协议状态信息。然而，Babaioff等[8]证明了在点对点层的信息传播并不总是与激励相容。仍未知是否参与者内化足够的价值从点对点网络作为公共利益为传播信息的机会成本Babaioff等人,还是信息传播平衡在野外观察到(人们自愿参与点对点协议)是不稳定的,最终可能会分解。

Johnson等[59], [68]研究了对等协议的参与者是否和何时被激励参与网络级的拒绝服务攻击。他们的结论是，矿泉有动机发动攻击，大的池子比小的池子更容易攻击，大的池子比小的池子有更大的动力去攻击。在野外经常观察到对池的拒绝服务攻击，因此可以通过观察到的现象学来支持这一理论分析[120]。另一些则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]。

## Ⅳ.客户端安全

比特币的普及，使得有用且安全可靠的密钥管理对于一大批的新用户变得极为重要。不同于其他大多密码系统的应用，若密钥丢失或者被损害，用户将遭受迅速且不可挽回的货币损失。所以它是可用安全领域中一个令人兴奋和重要的研究部分。

### A．简易支付验证（SPV）安全

尽管参考比特币客户端维护的是整个区块链的有效副本，但这将对移动设备造成极大的负担。一个简单的观察导致轻量级的选择：假定大多数节点只在有效链（第Ⅲ节B中的正确属性）上挖矿，那么客户端只需验证工作的证据，就可以信任只包含有效交易的最长链。这样SPV验证[90]能够使不受信任的节点，有效地向轻量级客户端证明交易一个交易已包括在达成协议的历史里。

SPV 在以绝大多数移动的比特币客户端为基础的BitcoinJ库中被执行。尽管优化是有可能的，比如从硬编码检查点开始，SPV验证也要求处理不断增长的工作证明链。当SPV要求向第三方公开客户端感兴趣的地址集时，它也带来了隐私问题（见Ⅶ和[49]）。

### B. 密钥管理

当几乎所有其他形式的网络商业都依赖于密码或者机密信用信息时，比特币依靠公钥密码来进行用户认证。比特币软件的开发者尝试了各种方法，以解决或者至少掩盖长期存在的密钥存储和管理的使用问题。Eskandari 等人[43]为比特币密钥管理接口的可用性提出一套评估标准，并且得出了如今的工具使用了不能完全捕获密钥管理行为的含义的复杂隐喻的结论。

**存储在设备上的密钥。**直接在磁盘上存储一堆密钥是最为简单的模型，但是密钥可能被专门设计的恶意软件窃取[75]。一些客户端在向新创建的比特币地址发送更改，被要求每次当前密钥池被耗尽后都要生成一个新的备份（通常在发生时没有出现任何用户界面提示），而其他一些用户向原始地址发送更改，或者导出从单个随机种子导出所有密钥。

**拆分控制。**为了避免单点故障和增强安全性，比特币可被存储在有特定n个公钥的k-of-n多签名脚本中。为了兑现脚本，k个有效的签名必须从这n个密钥中被提供。一个简单的例子就是一个钱包，它在发送资金之前需要用户的笔记本电脑和手机的同时签名。又或者，资金被存储在单个公钥下，但该密钥的共享需要使用门限加密技术被分配在n个当事方之间[50]。

门限签名实现了相同的k-n安全性，但它看起来像在区块链上正常的P2PKH交易，并且保持参数k和n的私有。

**受密码保护的钱包。**比特币客户端可以允许一个存储的密钥池文件（称为一个钱包）使用由用户选择的密码导出的密钥进行加密。受密码保护的钱包阻止某些确定类型的盗窃，另外，如果文件是物理或数字被盗，还需要密码猜测或击键捕获。受密码保护的钱包可能会误导用户去相信密码本身就能为在新设备访问资金提供通道。

**密码衍生的钱包。**密钥池可以从单个用户选择的密码中被确定地导出，且若密码能够被内存记住，那么跨设备使用可被实现(这种方法通常称为脑钱包)。非节流穷尽的常见/弱密码的搜索是可能的----彩虹表已经在区块链上揭露了未得到充分保护的比特币地址。另外，一个忘记的密码将使所有关联的资金无法撤回。

**离线存储。**钱包在无源便携式媒体，如纸张或者USB储存器等进行离线存储，能够增强对来自恶意软件的威胁的防盗保护，并提供了熟悉的物理性保护的心理模型。然而，当密钥池耗尽时，它们必须被更新。至于纸质钱包，以可扫描形式被打印的私钥(如QR码)可能通过钱包的被动观察而被窃取(如在直播电视上[101])。最后，离线钱包最终必须向使用设备加载密钥，这是最易受恶意软件攻击的时间点。

**空隙和硬件存储。**空隙存储是一种特殊情况下的离线存储，在这种情况下，持有密钥的设备可以执行计算，如为其持有的密钥签名交易。空隙存储能够通过不将密钥直接暴露在网络连接的设备上来阻止某些确定类型的窃取。也就是说，未经授权对交易签名的Oracle的访问与访问密钥本身并不是完全不同——两者都允许窃取。硬件安全模块(HSMs)通过将密钥材料从主机设备中分离出来，从而模拟气隙的特性，并且只暴露了签署事务的能力。

**寄存钱包。**第三方Web服务通过标准的web身份验证机制，如密码或双因素身份验证等提供密钥存储、管理和交易功能。这提供了最接近传统网上银行的服务，然而它要求信任主机。大量由寄存钱包造成的窃取[41]或破产[86]被中被记录的事件，已达40多起，涉及金额超过B1000。

## Ⅴ.修改比特币

现在，我们将重点转移到比特币的修改和扩展上。在本文的剩余部分，我们将评估和比较已被提出的更改。而在本节中我们将讨论实施更改的可用机制。

### A.比特币本身的升级

我们可以区分以下级别的变化

* **硬分叉。**若协议使得将被视为无效的交易或区块在先前的规则下启用，比如增加块奖励、更改已分配的块大小限制或添加新的操作码，那么该协议的更改就要求硬分叉。如果矿工更新到新协议，他们可能会产生被其他节点拒绝的区块，导致一个永久的(因此是“硬”的)分叉。所以，涉及硬分叉的更改需要在实践中接近完全一致地尝试。
* **软分叉。**与硬分叉相反的，软分叉的更改是与现有客户端向后兼容的变化；通常，这涉及被认为有效的块或交易的限制。这样的改变只要求大多数矿工同意升级的支持，因为老客户继续考虑其有效的区块。不升级的矿工可能会通过产生其他网络认为无效和可忽略的块，来浪费计算工作，但总是会重新加入大多数矿工发现的最长的链。这使得引进软分叉更改比硬分叉更安全。在一些情况下，软分叉可被使用来把新的操作码引入脚本语言。这是可能的，因为当前存在几个未被使用的操作码，它们被认定为无操作数；包括在交易输出中的操作码都可能使其由任何人使用，因此它们通常被避免。然而，如果矿工决定去拒绝该操作码所指示的某些条件下已显示失败的交易，那么这些操作代码中的任何一个都可以被赋予新的含义。这是对可接受交易集的严格限制，因此只需要一个软分叉。回顾过去，将所有未使用的操作码在最初作为无操作数，并通过软分叉提供最大的灵活性去引入新的更改，是较为明智的做法。
* **中继策略更新。**回顾Ⅱ-B3，节点在其将中继的内容中执行比实际能够有效接受的更严格的策略。更改该策略或在通讯网络的绝大多数其他方面都需要最小的协调，因为它们通常可通过向后兼容的方式被进行,并用节点通告他们的协议版本号。默认的中继策略已进行了多次更改以添加新标准下的交易类型，比如多签名事务。

### B.替代数字货币Altcoins

由于没有硬分叉的比特币更改的程度有所限制，数百种衍生系统，也就是指替代数字货币，随着代替的设计方法出现。其中的许多个系统已经分叉出比特币的代码库并维护了它的大部分特性，尽管有些系统(如Ripple)是完全独立的设计。替代币必须引导货币的初始分配，以吸引用户的参与，而这可通过以下几种方式实现：

* **新创世块。**替代币仅仅是从零开始建立一个新的区块链，向最初的矿工分配资金，就像比特币早期所做的那样。现在，隐货币共同体看待这种途径较为谨慎，因为发起人发行了一波钱币，并希望通过早期开采来获利。16
* **分叉比特币。**为了避免创始人享有特权，替代数字币可能会故意在某一时刻，选择去分叉比特币，接受先前的交易历史和资金所有权。比特币所有者在最初的系统中将继续持有比特币，并在其成立时加上同等数量的新货币。从技术上讲，这工作时完全像是硬分叉，只是没有宣称分叉是合法的比特币区块链。有趣的是，这一做法似乎还没

16对于比特币本身，中本聪(Satoshi Nakamoto)是唯一的矿商，至2011年该公司积累了超过1百万英镑，其中大部分仍未使用。

有进行认真地尝试。

* **烧录证明。**一种更流行的继承比特币分配的方法是证明烧录[113]，其中用户必须证明销毁了一定数量的比特币，这通常是通过将比特币中的资金转移到一个无法找到私钥的特殊地址，比如带有所有零哈希的密钥。这种方法的缺点是永久性地降低了比特币在流通中的数量。
* **楔入式侧链技术（pegged sidechains）。**最近，一些较有影响力的比特币开发者[9]提议侧链，使得比特币可转让并最终赎回。添加验证规则以从一个侧链兑换货币，将需要至少一个软分叉的比特币。

替代币还必须与比特币来竞争矿商(并避免比特币矿商们对金手指的攻击)，但在货币达到非零汇率之前，这可能是很困难的。一种流行的方法是合并采矿，即若替代币的根被包含在有效的比特币块中，就接受块，因此使得比特币矿工能够在替代币中开采块而不执行任何另外的工作。这可以迅速提供比特币的全部挖掘能力给替代币，正如许多比特币矿商将大量的替代币合并，以获得额外的回报。然而，它阻止了替代币偏离比特币的计算谜题。

## Ⅵ.备选的共识协议

比特币的共识协议一直是它最受争议的组成部分，原因是关于稳定性的公开问题(见Ⅲ-B)，以及对该协议的性能和可伸缩性的担忧[112]，并担心它的计算谜题浪费资源。在本节中，我们评估备选的方案以寻求共识，注意到在每种情况下，对稳定性的影响在提议的更改都是未知的，而备选方案几乎不规定它们宣称会提供的明确的稳定性性质。

通常，备选的共识计划的目标是用比特币确定一些明确的可察觉的问题，并希望比特币的稳定性问题能够得以延续，尽管由于缺乏一个可靠的模型来保证比特币本身的稳定性，这可能是一个不可靠的假设。

### A．参数更改

比特币的共识协议包含许多“魔法常量”，它们是基于最初的猜测工作硬编码的。几乎每一个的替代币都至少包含一些不同的参数，但这些更改往往是有争议的。我们仍然只有几个明确的指导方针，关于如何选择这些参数以及它们如何影响稳定性。

**块间时间和难度调整窗口。**比特币会自动调整其计算谜题的难度，为了（平均）每隔10分钟就找到解决方案。此设置主要受网络延迟的限制；若解决方案的速率太高，那么矿工在增殖之前会频繁地查找冗余块。另一方面，较慢的块速率直接增加了用户等待交易对确认所需的时间。比特币的设置是对所有账户保守的；我们所知的所有替代币都有相同的速度或更快(莱特币Litecoin，第二大流行系统，比比特币快4倍)。有许多建议去更改通信网络的各个方面以减少延迟，允许此参数安全地减少[38]，[73]，[112]。

**对块和交易规模的限制。**最有争议的更改之一是提高块规模的1MB限制[3]。随着交易量继续稳步增加，这一限制可能很快就会经常性达到。交易量的上限至今仅为每秒7次，大约比Visa网络的峰值容量小1000倍[53]。一旦达到此限制，交易将需要有效地使用他们的费用来为稀缺的资源出价。这可能会提高比特币的使用成本，可能会减慢采用率，但能够增加矿工的收入。它还可能导致用户依赖对链外交易的进行汇总和结算的中间方。限制是人为的，并且网络的带宽可能维持增加的态势；另一方面，增加的交易量可以排除一些受带宽限制的用户。虽然我们的知识都还没有接近实际利用这一能力，所以它将如何影响系统的运作仍然未知。

**货币政策。**比特币的共识协议通过新货币铸造的汇率和汇率变化的时间表，有效地授权了货币政策。比特币通过授权限额的货币，有效地制定了通货紧缩的货币政策，这使得多名经济学家预测该系统最终会受到通缩螺旋的破坏，从而没有人愿意花费比特币，因为囤积这些比特币被认为是更有利可图的[52],[65]。硬币的发行是变化最广泛的参数之一：例如，对于狗币Dogecoin，通货膨胀将无限期地继续，但对于弗雷币FreiCoin，通货膨胀率将以和谐递减的速度进行[116]，通货膨胀率将永远保持不变。

### B．替代计算谜题

Miller等人[85] 展示了一种用于比特币兼容的工作量证明的设计的方案，该方案被称为擦除谜题，其本质上必须分解为单独个人的尝试。这个属性常常被称为“无进展”的谜题。这确保了每个块的创建者通过计算功率的加权随机采样来选择，即使小的参与者也能够因为他们的贡献而获得(成比例的)奖励，并且连续的谜题解决方案之间的时间足够充分来使得谜题的解决方案得以传播。进步-自由是必要的，但不足以达成最终的共识协议来实现公平。比特币的SHA-256谜题是没有进步的，但其他许多的结构是可能的。

**抗asic难题。**虽然比特币的挖掘最初是通过使用通用处理器来进行，但挖矿的竞争性导致了更强大、更节能的定制硬件的稳步发展。如今，ASICs占比特币计算能力的绝大部分。泰勒提供了一份对高效率地计算SHA-256的技术挑战的出色的调查，并估计今天的ASICs已经在理论效率极限的数量级之内[115]。

比特币挖矿远离核心的民主价值（即“one-CPU-one-vote”[90]）通常被认为是消极的，因为系统中的大多数参与者没有自己的ASICs，并因此不再执行挖掘。有许多针对ASIC-抵抗的挖掘谜题的建议被提出。在理想情况下，ASIC-抵抗的难谜题可通过使用商用硬件来有效地解决，并且对于定制硬件只需具有较小的性能增益。迄今为止采取的主要方法是设计“memory-hard”谜题，其被设计为要求对大内存的有效访问。迄今为止最流行的memory-hard谜题(用于Litecoin和Dogecoin等)是scrypt散列函数[96]，这最初被设计用于抗破解密码散列。直到2014年，是否有可能设计一个谜题，它很难被memory-hard计算却很容易被memory-easy验证，这仍然还是未知的。Tromp’s cuckoo-cycle 谜题[117]似乎肯定地回答了这个问题。若ASIC-抵抗是有可能，它仍然是一个有争论的重要问题。17例如，ASICs已经在市场上发布，并提供了与ASICs相媲美的性能提升。但ASIC-抵抗的可取性是不确定的。Asics意味着从商品设备中窃取周期循环的僵尸网络攻击不再与现代挖矿平台竞争[57]。依赖于未来的比特币计价挖矿回报的大型矿商，期望收回他们在无其他价值的对ASICs上有特定目标的投资[23]，他们也可能有更强的抑制攻击的因素，正如Ⅲ-B2节中所讨论的。

**有用谜题。**通过计算谜题达成共识表现出在计算上消耗的能源和用于制造挖矿设备的能源和资源都是浪费的。若有可能在利用这项工作以达到某种目的，同时保持相同的安全级别，那么其中一些废物将可被回收。Becker

17这个问题在其他应用程序中也有应用，包括密码散列和密码加密，当前的密码散列竞争正在试图确定一个新的标准。

等人[14]也假定比特币最终可能被控制世界能源供应的现实世界实体所支配。

一个常见的建议是使用搜索功能去将其应用于科学研究，正如流行的Folding@Home[67]项目。对于有用的谜题，它们的一个挑战是他们必须被自动生成并与没有受信任的当事人进行验证，否则该方可以选择他们已经开始的谜题。Kroll等人[64] 进一步指出，任何有用的难题都必须产生一种纯粹的公共利益，否则它可能通过取消回收效果来恢复开采量的方式导致增加其开采量。

Primecoin [62]引入了第一个在替代币上的有用谜题。它的谜题要求找出大量数学上感兴趣的素数序列，这些序列可以作为密码协议的参数。Miller等人[83] 提出了一个包含可检索性证明的谜题，以至采矿要求存储大量公共数据集的一部分。特别地，若公共数据集对比特币网络本身有用(如区块链历史)，则这种方法提供额外的激励措施去为网络提供资源。

**不可外包谜题Nonoutsourceable puzzles。**大型矿池的增长及其促进共谋和联合形成的潜力，推动了不可外包的谜题的设计。同一个池的成员并不直接信任对方；但是这些联盟成功了，因为成员很容易去证明他们在执行挖矿的任务，并且如果成功的话，他们将向矿池管理者支付报酬。Miller等人[85] 以及Sirer和Eyal[111] 已经提出了“不可外包”的谜题，以确保无论谁进行采矿工作，在发现一个区块时都可以为自己争取回报，因此限制了矿池的执行机制，这使得匿名参与者之间不太可能形成大型矿池。

### C．虚拟挖矿和权益证明

在高层次上，工作量证明谜题的存在需要花费资源来进行开采。不是让参与者通过将财富交换为计算资源(再将其交换为挖矿奖励)的方式“挖矿”，而是有可能让他们直接将财富交换为选择块的能力。随机样本不是通过随机抽样的参与者的计算能力来推动全球历史，而是通过当前的财富分配来加权。我们可以称这种方法为虚拟挖掘。它有时也被称为“权益证明”[98]。

虚拟挖矿的好处主要有两个方面：第一，对攻击者而言，获取大量数字货币可能比获得足够强大的计算设备更困难。第二，通过避免消耗实际资源(即计算周期)，不会浪费任何真实世界的资源。迄今提议的虚拟采矿有几种不同的方式，这些方法主要依赖于拥有一定数量的货币拥有量使一个人有资格选择下一个区块的标准：

* **货币年龄证明。**点点币Peercoin[63] 张贴交易(很可能是针对自身，在这种情况下货币不会丢失)来证明拥有一定数量的货币来进行采矿。每一种货币的数量是通过它的货币年龄加权得到的，这就是货币自从最后一次移动以来的时间。
* **存款证明。**在Tendermint [66]，参与采矿要求在时间锁定的结合账户中存放货币，并且在采矿期间它们不能被移动。
* **烧录证明。**Stewart [113] 提出通过销毁硬币(将它们发送到不可用的地址)来进行挖矿。
* **活动证明。**Bentov等人[20] 提议让每个货币所有者默认地无保留地进入挖掘彩票；定期地，使用来自信标的随机值(如从网络上发生的交易中产生的值) 去随机选择系统中的所有货币；获胜货币的当前拥有者必须在一定时间间隔内用签名的消息作出响应。

这里还存在模型假设的形式化，这允许虚拟采矿系统实现安全性的，或可将虚拟采矿系统与共同设置中的计算谜题进行比较。Poelstra [97]展示了一个民间的争论，表明消耗外部资源（即燃烧能量）对于区块链安全是必要的，因此是虚拟开采方案本身是不可行的。其核心论点——被认为是无权益关系的问题——虚拟采矿易受成本较低的模拟攻击影响；没有什么可构成对货币分配不同的替代性的历史观点。为虚拟挖矿的稳定性或对抗稳定性提供严格的论据仍然是一个争论性问题。

### D.指定权威机构

尽管比特币分散的性质已经证明是一个有效的卖点，而且在许多社区中是一个被严格捍卫的原则，但如果我们能够依靠（少量）指定的机构接收、按顺序订购和签署交易，那么共识将大大简化。这将使稳定性假设更容易推理，并消除对浪费计算的担忧。Laurie [69] 首先建议使用指定权威机构的列表和标准的拜占庭协议。

与大型比特币矿商因其在未来汇率中所持股份而受到激励的观点类似，如果当局通过诚实的行为赚取少量收入，他们就不会有不当行为的动机。类似的选择也可以用来分配新的资金，以获得股权证明(Laurie最初的提议[69]在当局中建议买彩票)。对这些权威机构的信任可能会进一步受到限制，因为使用一组互不信任的权威机构[69]，使用社交网络选择哪些权威机构信任[108]，或授权硬币所有者每次使用硬币时选择他们信任的权威机构[24]。Ripple[108]是与此模型一起部署的为数不多的alt硬币之一;然而，它的稳定论点仍然没有得到证实。

## Ⅶ.匿名性和隐私性

比特币提供了一个有限的不可链接性的模式：用户可以在任何时间轻易地创造新的化名（地址）。这就是说在原始规范下提供强大的隐私性 [90]，但是事实很快就变得很清楚，由于区块链的公共性质，则在假名之间跟踪资金流动是有可能，并得出它们很可能受到同一人控制的结论。[56]在本节中，我们将讨论了对比特币用户的隐私威胁和所提议的隐私加强设计。

### A.去匿名化

不可链接性的实际水平在很大程度上取决于我们所使用的术语的实现细节[80]。例如，商家在产生每个新交易的付款地址时确保收到款项不会自动链接在区块链。相反的，客户可能需要在他自己众多的地址中组合出支付账户18，并将这些地址(及其伴随的交易历史)链接到区块链上，因为不同的用户很少为单个的联合交易贡献输入19。诸如“每个非改变的输出由单个实体控制”[4]的其它习语和“地址至多改变一次后使用”[80]也可以被对手用于由同一实体控制的不同地址的链接。

链接可以通过过渡到产生地址串;这是事务图分析的一个实例。对对手的一个主要挑战是这些习语是易碎的:随着实现的发展，它们可能会产生误报并失去准确性。新的链接技术也会到来。例如，多签名地址对隐私会产生意想不到的负面影响，因为更改地址中的多sig结构可以与发送地址相匹配，即使涉及的键改变[50]。

至于去匿名化，对手必须采取进一步的步骤，将地址集群与现实世界的身份联系起来。Meiklejohn等人[80] 成功地确定了属于网上钱包、商家和其他服务提供者的集群，因为通过与这些实体互动的方式很容易获得至少一个与这些实体相关的地址。至于确定固定用户，作者建议，由于大多数流程都通过这些集中服务提供商（通常需要确认客户身份并保留记录），因此对于具有传票能力的部门来说，这可能是很容易的。然而，在没有这种

18另一种支付方式是使用多个不同的商家地址，以避免合并[54]，但这尚未标准化或通过。

19一个例外是VII-B中的CoinJoin，它明确使用多输入交易来增加匿名性。

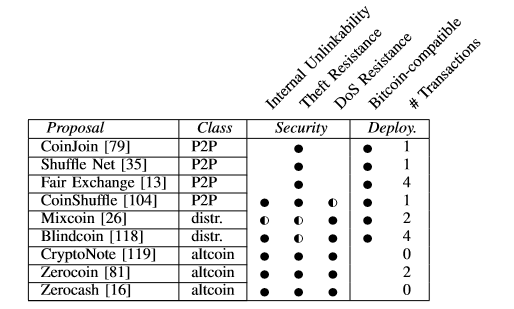
访问通道的情况下，对手就会受到限制，这是因为流量的中心性——网上钱包和其他类似服务将用户的钱币混合在一起。

**网络去匿名化。去**匿名化的另一个主要目标是对等网络。节点在广播交易时会泄漏其IP地址。所以，使用匿名网络对隐私至关重要。然而，Biryukov等人[21]指出一种DoS攻击能够在比特币网络中将Tor退出节点。比特币的P2P层能否更好地利用Tor，或者是否将开发一个专用的匿名网络，这些还有待观察。最后，由于难以隐秘地检索客户所感兴趣的交易列表，则当前的SPV实现方式提供了较弱的匿名性[49]。

### B. 提高匿名性的建议

这里有三种主要针对匿名性的提议。在表VII-A中，有针对五个安全和部署属性的比较（其中●表示该方案有一个属性，◐表示它有部分属性）。

**对等网络。**在P2P混合协议，一组比特币持有者共同创造一系列交易（私下）排列他们的硬币的所有权，使每个参与者在这一集群中匿名。这个过程可以在不同的用户之间重复，以增加匿名集群。

表Ⅰ 匿名技术的比较评估

实现这一目标的一个直接机制是混币CoinJoin[79]，如果一个集群的用户形成一个标准的比特币交易，其中每个用户输入一个输入，并控制一个新的输出地址，以致检查该交易的外部方不知道哪个输入对应于哪个输出(提供外部不可链接性)。如果用户期望的输出地址没有被包括，那么它们都可以拒绝签署该交易，这样能够防止盗窃，但使其容易受到任何个人的DoS攻击。在混币机制中，用户向其他用户通告他们的输出地址（不提供内部不可链接能力）。这可以通过切换新的TOR电路或其它自组织方法来实现。对于内部的不可链接性，匿名混币CoinShuffle [104]就是用于通过密码混合协议形成混币交易的覆盖协议。它还通过识别使交易中止的其他方身份，在一定程度上防止DoS攻击。

前两项提议提供了与混币CoinJoin相似的属性，其中一项基于改组网络[35]，另一个基于公平交换的[13]。然而，这两种方法都局限于两种混合，使得内部不可链接性无法实现。为了解决寻找双方混合协议的合作伙伴的困难，Xim[22]是一种去中心化的协议，用于通过支付矿工的三个阶段的费用来寻找混合的合作伙伴，以阻止拒绝服务的攻击。

**分布式混合网络。**在mixcoin [ 26 ]，用户向第三方混合发送标准大小的交易，并接收由拥有相同混合的用户提交的相同数量的货币。这实现了对外部实体和部分内部的匿名（◐），因为混合知道用户和其他用户之间的输出链接，但其他用户不知道。其他用户也不能破坏该协议。虽然混合可以在任何时间窃取比特币，但是可以使用签名的认证来识别欺诈混合(提供部分◐防盗)。虽然Mixcoin的认证和其他功能仍未部署，但这是最常用的第三方混合方案[88]。

Blindcoin[118]使用类似Chaum最初的电子现金建议的盲币扩展了mixcoin[28]。这防止了诚实但又好奇的混合学习到输入和输出之间的映射，并升级到完全的内部不可链接性，而代价是另外两个交易来发布和赎回盲目的令牌。

**具有集成的不可链接性的替代币。**零币[81]是一种具有集成的不可链接性的货币，使用比特币状的基础货币和匿名的成为零币的影子货币。用户仅以基本货币进行交易，但可以相对于所有零币的集合(比以上其它技术更大的匿名集群)，以匿名方式将基础货币兑换成零币并从零币中移出。这提供了强大的不可链接性，并且没有盗窃或DoS攻击问题，又不依赖除矿工之外的任何实体。然而，这是不兼容的比特币，且必须为替代币（或硬分叉）实施。pinnochiocoin [37]是使用了不同的加密结构的类似提案。

零钞Zerocash [16] 是一项更有力的匿名替代币提案。零钞Zerocash交易是一种特殊的零知识证明，称为snarks[17]，这能够完全不披露关于数额或收款人的任何资料(可能的公共交易费用除外)，从而形成一种完全无法追查的分类账，其中不公开披露任何信息。snarks是一种新的密码原语，没有任何实时部署到日期，并且需要受信任方的初始机密参数的生成；然而，最近的工作表明，该初始设置可以分布在一组相互不信任的各方之间[18]。

密文CryptoNote[119]是一种使用环签名的加密混合协议，它已经被用作几个以隐私为重点的货币的基础。用户可以通过在他们选择的k个硬币(可能是未用的)上提供一个一次性的环签名来发送一个货币，这些货币的功能是一个匿名集群。一次性属性确保双开销尝试可以相互链接，从而导致无效交易。交易规模在k中是线性的，即单个交易的匿名集群的规模。该方案的性能较好，但其匿名性弱于零币和零钞。

## Ⅷ.扩展比特币的功能性

虽然比特币可以简单地描述为一种数字货币，但在矿工的强制执行下，脚本语言的强大力量，使得两个或更多相互不信任的各方之间的许多其他类型的互动成为可能，否则就要求一个值得信任的中介机构。我们使用去中介这个术语是指设计交易的一般过程，它消除了对可信中介的需求。

### A.今天比特币的去中介化

比特币作为一个可扩展平台的程度常常被夸大。脚本语言仍然受到高度限制。然而，很多协议都被设计成去中介化，这可以用比特币当前的交易语义来实现。以下是我们确定了三种常见的去中介化策略：

**原子性。**在众多情况下，所需的安全属性可以被区块链提供的功能直接执行，一个事实是交易能够是原子性的，且在多方签名之前无效。CoinJoin [79]是一个简单的例子，在所有当事方签名之前，没有人能够交换参与者的货币。另一个例子是Hearn的“连续小额支付”协议[55]，这使得我们能够有效地利用带外通道，允许一方批准几乎持续的缓慢释放资金(如每秒一小部分)，以换取一些计量服务，如互联网接入。付款人可以在任何时候停止通过停止签署任何更多的交易的方式来结束该协议，此时只有一个交易需要张贴到区块链。另一个巧妙的协议是Nolan的原子跨链交换协议，它允许用户用两个链接的交易和原子安全性，在两个替代币之间交换货币[91]。

**押金**。在另一些情况下，当所需的安全属性不能直接强制执行时，比特币可以通过张贴保证金或债券来提供可接受的挽救办法，且只有在行为正确的情况下才能退还保证金或债券。该方法的一个实例是以Andrichowicz等人的多人彩票协议[5]。N个缔约方中的任意一个放置一个BK赌注，而一方(随机选择)与BKN一起离开。为了保证作弊的一方不会因为学习游戏结果而破坏游戏，并且能够有选择地中止协议，每个玩家都必须存入BkN 2。如果任何参与者中止协议，他们就会放弃他们的押金，而押金是用来补偿其他参与者可以赢得的最高金额。这种方法并不局限于彩票，实际上可以为任意多方的计算提供一个公平的概念。[19]。

**可审计性**。即使比特币没有被应用对抗不诚实的一方采取补救措施，但它在提供证据证明不诚实的一方有罪上，仍然可以发挥关键作用。绿色地址就是一个例子[58]，其中，具有众所周知的公钥的支付处理器保证绝不签署无效或欺诈的交易。从绿色地址接收事务的用户可以接受它(即作出不可撤销的决定)，然后等待它被包含在区块中。如果在某一点上交易被发布在区块链中发布的欺诈交易抢占，则用户可以轻松地获得服务器欺骗的可检查证据。在混币中也使用了类似的技术[26]，其中半可信方提供签字保证，并与区块链一起提供不可辩驳的不当行为证据。

### B.作数据存储的比特币

扩展比特币的另一种方法是只将比特币作为全球性的附加日志使用，任何人都可以改写日志。

**安全的时间戳。**由于区块链是只附加（模块叉）的，所以能够立即用作安全的时间戳服务[31]，这在各种安全协议中都很有用。任意数据可以通过几种机制写入区块链——社区更喜欢使用一个小型的可证明的不可花费的脚本，其中包括未使用的变量中的数据。20多个服务从用户收集数据，并由矿工强制执行）来将颜色从输入交易转移到输出交易。货币最初可能会被着色，其中包括来自任何被信任去给某些程序发行颜色的权威机构的特殊签名。这允许创建任意的代币，这些代币被用于两方或普通无色的比特

20烧录证明也是一个解决方案，但这是不可使用的，所以矿工不鼓励使用它。

币之间相互交易。彩色币已经提出了许多应用，如股票交易或产权。由于比特币矿工不执行彩色币协议，所以确认交易的颜色要求为所有先前的交易扫描区块链（排除SPV证明）。

彩色币以使用历史追踪blockchain功能为特征。在一般情况下，它已被观察到的每一笔交易的输出有一个独特的先前历史，这对于不同的用户均是有意义的，并且意味着从长远来看，比特币不能保证是可替代的[89]。

**覆盖协议：万事达币。**一种更灵活的方法是使用比特币的共识机制，但定义完全不同的交易语法(具有任意有效性规则)，并将其写入区块链上的任意数据。请注意，此设计消除了比特币的共识机制通常提供的正确性属性，因为比特币矿工将不知道新的交易类型。所以，无效的覆盖交易可能被发布，并且要求被覆盖系统的参与者忽略。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。两种主要的制度是合约币[39]和万事达币[123]，这定义了用于交易数字资产和合同的大量附加交易类型。

### C.扩展比特币的交易语义

比特币的脚本语言是故意限制性的；事实上，原始的源包含一个更通用的语言，但大多数的操作码被标记为不可用。在我们的论文的网络版全文[25]中，我们解释和评估各种建议，如域名币Namecoin [76]和Ethereum [125]扩展比特币的功能性来为去中介化提供了一个更为灵活的平台。

## Ⅸ.结论语

基于学术和（大量的）在线文献，我们对比特币进行了广泛的分析，其中显示出了设计一种实用的数字加密货币的新想法的复兴，这是对计算机社区安全的长期挑战。创新并不局限于新的数字加密货币协议设计，而是涉及计算机安全、分布式系统、硬件设计和经济领域的许多领域。这是一个丰富而深刻的空白部分，它不应该被简单地忽略，因为许多想法并不是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很大的增长，但我们的理解仍然缺乏。一个简单的事实证明了这一点:如果有机会从头开始设计货币体系，那么目前还不清楚比特币有多大的偏差，以及它们在实际操作中会产生怎样的影响。这并不是说比特币是完美无缺的，因为它有许多设计怪癖。还有一些领域，例如匿名，在这方面提出了明显优于其他的设计。然而，对于基本的稳定性和效率而言，是否有可能设计出一种可以改进比特币的分散共识系统，目前尚不清楚。这些文献甚至没有提供足够的工具来评估，在经济和社会假设下，比特币本身将保持稳定。同样，在设计具有新功能的非中介协议时，如何在不破坏其所观察到的稳定性的前提下扩展比特币的功能还不清楚。

总的来说，我们知识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使用不同参数或不同情况的问题。尽管有时对于在比特币社区的计算机科学学术研究感到担忧，但我们主张让研究发挥重要作用，而不是简单地“让市场来决定”。今天，要评估比特币相对于替代数字货币的成功程度是很困难的，因为比特币有具体设计选择，而不是它的先行者优势。

比特币是一种少见的实践超前于理论的情况。我们认为，这是一个为研究界解决大量关于已有比特币的仍有争议的问题的巨大的机会。

确认

作者想感谢以下同仁对本文草稿的反馈意见：Sergio Demian Lerner, Luke Valenta, Albert Szmigielski, Gus Gutoski, Ben Laurie, Ittay Eyal和

IEEE Security & Privacy的匿名评审员以及比特币社区的成员。Joseph Bonneau由 Secure Usability Fellowship支持. Jeremy Clark 由NSERC Discovery Grant支持. Joshua A. Kroll 由NSF Graduate Research Fellowship under Grant No. DGE-1148900支持. Arvind Narayanan由NSF Grant CNS-1421689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. SybilResistant 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,andR.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:Bitcoinprivacyfortherealworld. bitcointalk. 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 ScratchOff 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] QuantumMechanic. Proof of stake instead of proof of work. bitcointalk.org, July 2011.

[99] R.L.Rivest. Peppercoinmicropayments. InFinancialCryptography, 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.