迷你区块链协议

J.D. Bruce
July 2014. Rev 2.
March 2017. Rev 3.
www.cryptonite.info
Translated into Simplified Chinese from cryptonite.info/files/mbc-scheme-rev3.pdf
by www.xcnchina.com

摘要

几乎所有 P2P 加密货币都可以防止双重支付和类似的此类攻击，使用庞大的“区块链”方案，以及通常不使用某种形式的方案，管理交易的伪去中心化解决方案。在这里，我们提出一个纯粹的网络可以忘记旧交易的 P2P 加密货币方案。由于节点只需要区块链的最新部分才能与网络，我们称这部分链为“迷你区块链”。我们认为损失可以通过一个小的“证明链”来解决这个修剪过程产生的安全性问题，硬币所有权数据的丢失是通过一个数据库来解决的所有非空地址，称为“帐户树”。证明链保护小区块链，小区块链保护账户树。本文将描述这三种机制可以协同工作以形成一个系统的方式提供高水平的完整性和安全性，但比所有其他纯粹 P2P 货币。它还提供其他潜在的好处，例如更快的交易和更低的费用，更快的网络同步，支持高流量，更多阻止自定义消息的空间，甚至可能增加匿名性。

简介

五年前，“中本聪”首次向公共领域发布比特币并永远改变了许多人对金融和经济的看法 [1]。当时难度低，区块链很小。 头两年的事情看起来很棒，许多人认为区块链在很长一段时间内不会成为问题，所以这个问题被搁置一边。我们现在是 2014 年 7 月，区块链接近 20GB 大小 [2]。虽然仍然可以控制，但它正在成为一个令人担忧的严重问题。

比特币的核心开发人员现在将他们的大部分注意力集中在处理不断增长的网络流量上。 今天，bitcointalk.org 论坛几乎每天都在观察关于最小化区块链大小和减少同步时间。 迄今为止采取的最有效措施之一是从 Berkeley DB 到 LevelDB [3]。 BDB 慢得多，切换到 LDB 导致在同步和块验证速度方面的主要性能提升。

另一个有前途的努力是“终极区块链压缩”项目 [4]旨在通过实施区块链实现“接近最优的区块链压缩”修剪技术，包括“维护和验证的平衡树信息”通过合并挖掘在一个单独的区块链中”。区块链

修剪确实是一个有前途的可以证明可以提供高水平的压缩，但它增加了额外的一层复杂性，并不能以完全令人满意的方式解决所有可扩展性问题。
bitcointalk 论坛还观察到许多关于更改最大块大小限制的主题（有很多人支持和反对）。 一群反对改变的人发布了“比特币块大小问题视频” [5] 他们反对增加最大块大小因为“运行一个节点会变得更加昂贵”。 Gavin Andresen，比特币核心主管开发者回复：“区块大小会增加。 你的视频只会让很多人什么都不担心”。 这个问题似乎每天都变得更加紧迫。

最大块大小肯定会在某个时候提高，现在交易容量被限制为每秒 7 次交易 [6]，最终这不会是足够的。提高比特币的最大区块大小将需要协调的硬分叉，因为所有老客户都不知道如何处理更大的块。所以有合法的担心增加最大块大小的原因，但这并不意味着它不是需要。有几个必须考虑的缺点和优点。

增加最大区块大小会增加交易带宽并降低费用，但它会导致区块链增长得更快，并对节点施加更多压力。许多 bitcointalk 论坛的成员说，问题不是最大块大小，而是他们指责像 Satoshi Dice 这样的赌博服务向网络“发送垃圾邮件”交易。其他成员指出，Satoshi Dice “正在为网络，并表明除非取消区块大小限制，否则就会出现问题”[5]。

我们应该担心吗？

正如刚才提到的，有几种方法可以尝试处理区块链。 在 Bitcoin Stack Exchange 上，用户 Sean Chapman 问道：“有没有研究区块链随时间扩展的规模？”。Meni Rosenfeld，顶级作家
回答，解释说虽然他不知道任何符合查普曼要求的研究，但他可以概述我们不必担心区块链可扩展性的 5 个原因 [7]:
1. 并非每个用户都需要运行完整的网络节点。
2. 可以从区块链中修剪花费的输出。
3. 链下交易有助于减轻网络压力。
4. 交易费用可以抵消区块存储成本。
5. 在可预见的未来，摩尔定律依然强劲。

中本聪在 2008 年底谈到了第一点，当时他说随着网络的发展挖矿“将越来越多地留给拥有专业服务器群的专家硬件”[8]。这也许是一个令人满意的解决方案，但它会导致持续中心化，最终这些专家将控制网络的很大一部分通过使较小的参与者更难参与来增强力量。 第二点已经
提及；修剪提供了希望，但它是一个复杂的过程，而且结果有限。

诸如最终区块链压缩方案之类的提案的主要问题是很多由 Satoshi Dice 等服务产生的“灰尘”仍然堵塞了系统。比特币将交易联系在一起的方式使其无法达到我们真正需要加密货币的可扩展性。最后 3 点也有一定的道理对他们来说也是如此，但不管这些点如何，我们仍然坚持使用区块链永远不会停止增长，它仍然没有为我们提供一个真正轻量级的方案。

我们应该寻找创新的新方法来简明扼要地解决这些可扩展性问题和令人满意的方式。 比特币 Wiki 指出“每个区块的交易率都非常高大小可以超过半 GB”[6]。 比特币达到那个水平真的可行吗？网络流量并试图将其全部存储在不断增长的区块链中？ 对于硬币，例如比特币的高度中心化可能是最终唯一的解决方案。很明显，作为我们迈向未来，需要更好的解决方案。

可能性是比特币会在这里停留一段时间，任何新的山寨币都不太可能突然让比特币过时了。迷你区块链方案提供了更好的功能一些领域但也缺乏大多数硬币由于简单交易而具有的一些功能我们使用的模型。我们的目标是在中本聪的工作基础上创建一个开放和自由的市场竞争可以蓬勃发展的最佳加密货币。 这里提出的方案可以为我们提供真正新鲜独特的优势。

寻找解决方案

下面是一个类似的全新替代加密货币的提案比特币在许多方面，但在其他方面也大不相同。 这是非常困难的对比特币代码库进行任何重大更改，不幸的是以下方案是与比特币不兼容。 该方案通过以下方式消除了对完整区块链的需求取消链接事务，从而允许在足够的时间后丢弃所有事务通过，但这样做会从协议中删除脚本，这是比特币无法做到的。

本文中描述的建议解决方案来自于理解不同的区块链的目的，然后将该功能分离为单独的每个机制都经过优化以达到其目的。 区块链有 3 个主要职能。比特币区块链将这些功能组合成一个单一的机制，结果不能很好地扩展。它需要您存储大量并不真正需要的数据要永久保存。 打破区块链的功能是关键。

区块链的功能：
1. 协调网络如何处理交易
2. 封装保护网络的工作量证明
3. 管理账户余额； 记录硬币的所有权

由于该提案的原始版本是在 2013 年初编写的，因此它已得到改进并进行了重大修改 [9]。在其他 bitcointalk 论坛成员的帮助下，迷你区块链计划得到了充实，创建了一个项目 wiki 以扩展原始白皮书的想法，并使用了一种名为 Cryptonite 的新币方案[10]。 实施它的过程极大地帮助了微调支持迷你区块链计划的概念。

本质上，迷你区块链方案通过存储所有非空的余额来工作我们称为“帐户树”的结构中的地址，因此我们实际上不需要任何交易来计算任何给定地址的余额。 我们已经删除了脚本系统以及随之而来的联锁交易的整个想法，并用一个交易在帐户树上执行基本操作的概念要简单得多，例如“从地址 A 的余额中减去币并添加到地址 B 的余额中”。

交易中的输入和输出不指向其他交易，它们只是指向帐户树中的地址，因此交易不会以相同的方式链接在一起它们在比特币中，我们可以在一段安全的时间后丢弃所有交易（足以使秘密链攻击不可行，稍后讨论）。 和 Cryptonite 节点能够删除一周前的所有交易，但它们可以选择存储尽可能多的历史记录，整个链不太可能丢失。

帐户树

该提案从“帐户树”的概念开始。 为什么我们要记录每一个如果我们只需要知道所有非空的余额，则将其永久保存地址？区块链的第三个功能被账户树取代。帐户树本质上可以被认为是分散的“资产负债表”。 它会包含每个唯一的非空地址和所有这些地址的余额，以及其他一些使提款限制成为可能的字段（稍后会详细介绍）。

当地址余额发生变化时，我们需要做的就是更新帐户中的数字树，而不是向其添加新数据。 当然，这不会提供真正有限数量的要处理的数据，因为新的非空地址将一直出现，但它尽可能接近有限。它在某种意义上是有限的，因为硬币将具有有限的可分性，我们不能真正期望世界人口或数量的互联网用户继续永远增长。 在任何情况下，它都是可扩展和可管理的。

即使有 100 亿人口，每个人都有 10 个不同的非空地址，我们只需要跟踪 1000 亿个地址。由于我们可以删除数据库中的空地址，因为交易只需要对等方在此数据库中移动数字而不是向其中添加新数据，帐户树应始终保持相当小。等到我们接近 1000 亿个唯一的非空地址，我们的计算机会快得多。

账户树中非空地址的所有者用他们的私人地址证明他们的所有权钥匙。像比特币一样，交易被创建为一组签名的数据并通过网络广播网络。 像比特币一样，接受交易的矿工然后将其放入他们的区块中致力于解决一个困难的问题，使其进入迷你区块链（更多信息请参见下一节）。接受区块的节点将更新自己的账户树副本通过转移硬币或做任何必要的事情。

建议的数据库被命名为“帐户树”，因为它应该有一个哈希树结构体。树中的每个“帐户”都有一个相应的哈希值，并充当树的底部。 作为一个哈希树，我们可以结合每个账户的哈希来构建一个哈希金字塔并计算顶部的“主哈希”。请注意，“帐户”不是像“比特币账户”这样的地址集合。在这种情况下，每个帐户仅指一个地址或叶节点（显然正常的“帐户”也会存在）。

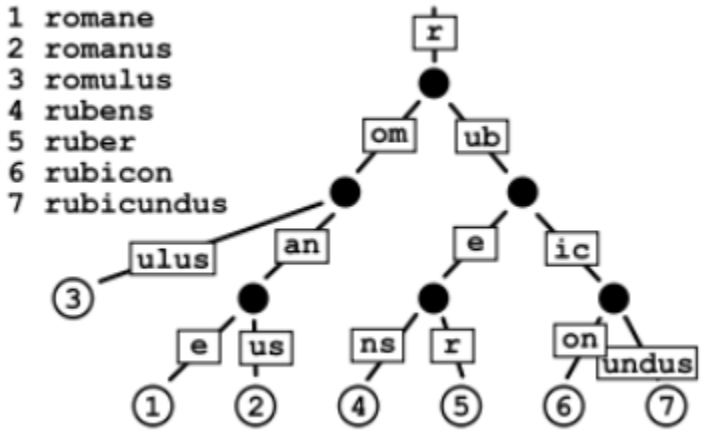

Figure 0-a

图 0-a 显示了一个通用的基数树/trie 结构（来源：维基百科）。实际上是 Cryptonite 使用一种结合默克尔散列的二进制基数树。什么没有显示在图是节点是如何散列的。 所有散列一起产生主散列/根哈希在顶部。即使树中只有一个帐户，主哈希也会改变以任何方式改变。 这个哈希

树系统为我们的数据提供了完整性，因为主哈希也存储在块头中，因此树受到区块链的保护。

使用二进制基数 trie 结构的优点包括:
- 它非常适合查找地址（公钥哈希）
- 它比许多其他树结构更快，内存效率更高
- 可以验证树的小部分而不是整体，并且可以证明完整性
- 以任何顺序将相同的数据插入到 trie 中将始终生成相同的结构

迷你区块链

迷你区块链提供了我们的第一个区块链功能。迷你区块链是本质上只是一个普通的区块链，除了我们不需要保留历史数据的副本块。同样，它并不是真正有限的，因为改变最大块大小可能会增加迷你区块链的平均大小。在本文的后面，我们描述了一种机制动态确定的最大块大小，但它不是方案的必要部分。

如果我们要使用一组节点哈希和一个主哈希来跟踪我们的数据库，我们不能允许每个单独的事务按需更改数据库。 我们必须将它们分解为定期插入数据库的事务组时间间隔。 无需将交易以块的形式在交易组中解决我们没有可行的方法来维护帐户树。这产生了对一个区块链，但由于我们可以丢弃旧块，因此我们将其称为“迷你区块链”。

比特币需要完整的区块链，因为这是确定完整区块链的唯一真正方法所有地址的余额。 然而，我们有帐户树来完成任务管理帐户余额并记录硬币的所有权。我们不需要完整的事情，我们可以扔掉旧块并节省大量磁盘空间。然而我们确实保留了几百或几千个最新的区块，这就是我们的迷你区块链。 迷你区块链还为我们提供了一定程度的安全性。

每个区块的头部都嵌入了主哈希，我们可以验证区块中的每个区块迷你区块链从头开始，确保每个区块中的交易始终对应于前一个块中的主哈希。因为有工作量证明每个区块在被接受到迷你区块链之前所需的过程，它攻击者很难生成假的迷你区块链。虽然很难，如果我们完全删除旧块，那绝非不可能。

使用比特币，我们可以从头开始，一直工作到最新点因为我们有完整的区块链。 如果攻击者从最旧的区块可用，新节点很难将它与真正的迷你区块链区分开来，因为在那个最旧的区块之前，它们没有发生过的历史。这攻击者可以花费尽可能多的时间来建立他们的累积难度迷你区块链，因为它不是一个他们必须超越的不断增长的链。

然后攻击者可以开始广播假链，它可能会传播到足以有成为主链的风险。 证明链通过提供一个可以充当存储长期工作量证明历史记录的容器的机制我们可以计算任何链的总累积难度。而不是完全删除旧块我们必须维护块头，以便我们始终可以跟踪历史任何给定的链并比较每个链的总累积难度。

证明链

证明链，它提供了我们区块链的第二个功能，本质上只是一个区块头链。 当节点丢弃旧块时，它们不会丢弃该块标头，只有交易。所以基本上迷你区块链是一个区块链但最近的交易。这意味着所有节点仍然可以使用区块链头来验证累积难度最高的最佳迷你区块链，感谢帐户树，他们不需要旧交易来计算地址余额。

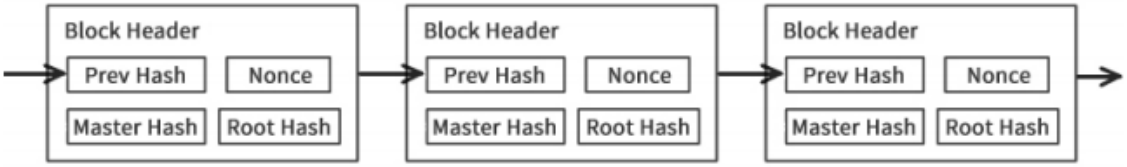

Figure 1-a

我们拥有本质上是普通区块链的东西，因此挖矿可以像它一样工作在比特币中。节点必须散列区块头并在下面搜索结果散列当前目标。可以丢弃旧交易并只存储一个区块链标头，因为证明解决方案不依赖于了解堵塞。 它是安全的，原因与比特币是安全的相同，证明链中的每个证明都提供进入下一个证明，几乎不可能生成假证明链。

主哈希需要位于图 1-a 中详述的区块头中，因为它允许验证区块中交易的节点，并确保他们的账户树已经块正确更改。存储在区块头中的主哈希计算后区块中的交易已被应用到账户树中。我们可以按自己的方式工作从证明链的开始到它进入迷你区块链的位置，我们可以验证我们拥有的最新区块是否有效。

证明链证明哪个迷你区块链的计算时间最长后盾。攻击者不再需要永远坐在那里生成假证明链，因为证明链必须输入迷你区块链。所以现在如果攻击者试图创建一个完全无效的迷你区块链，他们还需要一个强大的证明链伴随着它。这基本上将我们带回了典型的完整提供的安全级别。区块链方案，但它仍然不是在所有情况下都完全安全。

主要问题是攻击者可以秘密地建立在合法的证明链上使用无效的账户树，然后当他们认为时间太长了，没有人会将历史追溯到那么远。在那种情况下新节点将无法检测哪个链是真实的。我们称之为“秘密链攻击”。如果一周后可以丢弃所有交易（如在 Cryptonite 中），则攻击者必须保持大部分散列能力超过一周（秘密）。

我们相信，即使这种攻击确实发生了，也不会是灾难性的，因为：
1. 攻击只会影响超过一个时间没有与网络同步的节点一周，所有其他节点都可以检测到攻击并拒绝假链。
2. 新节点可以检测到正在进行的可能的秘密链攻击，尽管他们不知道哪条链是真正的链。
3.“社区检查点”的发布可以将节点指向正确的链中这次攻击确实发生了非常不可能的事件。

网络行为总结

网络同步

网络同步分 4 步实现：
1. 获得累积难度最高的证明链。
2. 获得与证明链相关联的迷你区块链。
3. 通过请求切片和验证哈希来构建帐户树。
4. 使用最近的交易完成账户树的同步。

首先，节点将使用“头优先”的方法来定位具有最高累积难度。然后它将获取最近连接的块的集合到那些块头。然后它会尝试获取账户树的切片，直到它有一个完整的树。账户树结构允许节点证明它已经收到完整的切片，以便节点可以确保它拥有所有帐户。最后，节点可以使用最近的将树的所有切片更新为最新的主哈希的事务。

不需要存储旧账户树数据，但节点必须构建账户树这与他们拥有的主哈希完全一致；他们不能混合和匹配切片与不同的主哈希相关联。这就是为什么每个切片的高度必须是确定，以便我们知道在步骤 4 中需要应用哪些事务。由于所有切片包含主哈希，当节点请求特定切片时，它可以匹配该切片通过比较哈希值来针对特定块。

节点通常会尝试获取在变得安全的点附近同步的切片丢弃旧的交易。其他节点能够提供这些旧切片，因为他们可以撤消最近对帐户树的更改并根据请求生成旧切片。新的节点将尝试在如此旧的时间点构建帐户树，因为它们需要能够创建一个大型“反转数据库”，其中包含撤消对帐户树，这对于生成旧切片和处理分叉很有用。

简单来说，新节点将尝试围绕该点构建一个完整的账户树在可以修剪旧块的地方，它将使用来自最多的交易“快进”最近的块，同时建立一个反演数据库，使其具有反演回到不再需要反演的点。当然这个描述这个过程非常简单，你必须阅读 Cryptonite 的源代码对同步如何工作的更详细的技术理解。

请注意，此过程不依赖于对块的大量检查，人们信任块他们有，因为证明链支持他们。验证证明链非常容易一旦完成，节点只需要确保它获得的块与证明链。随着帐户树的建立，唯一重要的是它最终拥有最新区块的主哈希。一旦完成并且节点是同步它可以通过接受有效块开始正常更新帐户树。

交易

比特币通过读取区块链来跟踪地址余额发生了什么，它是一个连续的分类账，而不是一个独立的资产负债表。比特币交易使用的系统包括“输入”和“输出”以及大多数新的输入交易通常参考之前交易的输出。迷你区块链方案使用基本的输入和输出概念，但输入指向帐户树和输出也指帐户树中的帐户。

输入账户将为发送到输出账户的硬币提供资金。这个操作会导致输入账户余额减少，输出账户

余额减少账户增加。费用仍照常使用，以优先交易和激励矿工。显然，如果交易不应该被接受为有效将任何帐户的余额减少到 0 以下，或者如果它请求任何与任何余额的价值，或者它尝试任何它没有权限做的事情。

为了确保相同的签名交易不被网络处理超过一次，交易还必须包含一个“lockheight”字段。交易无效一旦锁定高度超出节点需要保留的块范围（让我们调用这是“在视图中”的块），并且相同的 txid 不能在任何块中包含两次正在考虑中。这使得不可能两次使用相同的 txid。然而这解决方案要求 txid 不可延展。

尝试解决事务时需要考虑几件事延展性，但最重要的是我们不能在散列时包含签名交易，因为使用相同的密钥签署相同的数据会产生不同的签名每一次。发件人将签署 txid，但多次签署不会改变 txid，只有签名。因此试图改变事务的内容总是更改 txid 并因此使签名无效。

帐户树

帐户树有多种实现方式，但数据结构必须满足某些要求：
1. 所有数据都应该能够通过确定性哈希（master 哈希/分类帐指纹）。
2. 高效支持添加账号、修改账号、删除账号 4 种操作查找帐户。
3. 每次修改后都应该能够有效地更新帐户树主哈希。
4. 应该允许有效验证账户子集的正确性无需下载整个结构。

当硬币被发送到一个新账户时，新账户作为叶节点插入不存在的地址，当地址为清空。当地址确实存在时，交易将简单地改变现有帐户特里。迷你区块链在树更新时进行协调。当一个节点接收到一个新块，他们将通过更改来执行块中列出的交易他们的帐户树相应地。

提议的帐户树结构允许将所有地址余额汇总在一个“资产负债表”格式并允许所有节点安全地丢弃旧交易。但是，没有办法协调帐户树的更改时间和方式，我们仍然无法保证节点间的一致性。这就是迷你区块链的用武之地。当一个新块被接受到迷你区块链中时，节点将使用该块来更新他们以一致和协调的方式复制帐户树。

在分布式网络中，目前不可能每个节点都应用事务它看到了他们。事务必须连接在一起并批量应用。这样的清单交易组合在一起形成一个块，并与标题一起形成区块链。节点收集交易并将其应用到账户树以实现新账户树状态。新树状态的主哈希包含在块头中。其他节点接收此类块的人可以自己重放交易并检查哈希匹配。

讨论新的网络协议

动态最大块大小

正如本文引言部分所指出的，有很多关于最大块大小。一个值得讨论的潜在新网络协议是这个想法动态最大块大小。它可以是一个浮动值，也许由几个因素。我立即想到的两种方法是 1) 基于挖掘的投票系统和 2) 一个分析一些先前区块的系统和计算平均块大小以导出新的块大小限

制（例如 2*average）。

投票系统听起来可行，它可以让我们通过以下方式管理最大块大小群体共识，但它赋予矿池等群体很大的权力块大小将是。更好的解决方案是简单地计算某个数字的平均大小
最近的块，然后乘以某个值以得出新的最大块大小，有一些任意的下限。这样我们就不需要将所有投票数据存储在块。这是我们决定采用 Cryptonite 的方法。

即使使用我们的轻量级方案，也确实需要一个最大块大小，因为我们的网络在几乎停止工作之前只能处理这么多流量。即使是有限的区块链它可以随着足够大的块快速增长。然而在未来我们可能能够处理更大的块，所以我们需要一种逐渐改变的方法随着时间的推移。如前所述，硬分叉不是很方便。一个自动化的调整系统将是自我调节的，并且更加无缝。

修剪帐户树

迷你区块链方案中最庞大的部分实际上是帐户树。给够了帐户树可能会被许多低余额帐户填满如果我们可以在帐户陈旧后从树上修剪这种类型的“灰尘”，那将是有利的足够的。有几种方法可以实现这一点，但没有一个是远程简单或易于实施。最好的方法似乎是你收集
在帐户树中维护帐户的“帐户维护”费用。

从账户提款时将收取费用，并包括以及交易费用。费用将根据发送的年龄计算帐户。通过这种方式，低余额账户最终达到余额 0 并被修剪从树。即使没有从账户中提款，我们也可以有一个系统允许修剪那些将有非正余额的账户支付他们的账户维护费。

这种类型的系统的好处是它会在帐户树中存储数据，这在经济上是有益的，它有助于保持帐户树紧凑。另一个该系统的有用功能是我们可以将维护费用反馈给“coinbase account”（支付区块奖励）并确保区块奖励永远不会到达 0，实际上没有增加货币供应量，只是通过回收硬币通过采矿系统，在不切断铸造过程的同时保持有限的货币供应。

提款限额

在这个方案中，可以很容易地为个人账户设置提款限额，因为我们资产负债表方法。提款限额规定了最大数量的硬币每个区块都可以从账户中提取，这对几个不同的原因。需要在帐户结构中添加三个额外字段才能实现此目的：1) 上次修改帐户的时间（这对于修剪帐户树也很有用）2)当前提款限额 3) 潜在排队提款限额。

该限额由账户所有者使用特殊交易和默认值自行设置新账户的提款限额是无限的。提款限额的主要目的是帮助防止双花并使商家对与确认数量少。如果他们知道只有一定数量的硬币可以
每个区块从账户中提取，然后他们就知道即使是 0 确认交易可能会通过，因为攻击者不能一次取出他的所有硬币。

提款限额如何运作的简要概述：
1. 向网络发送特殊交易修改您的提现限额帐户。限制被指定为每个块的硬币数量，并保存到队列中场地。此类更改将在例如生效。100 个块，之后排队 value 覆盖实际提款限制值。
2. 网络接受特殊交易，100 个区块后拒绝任何交易会导致超出新指定限制的交易。

商家可以通过以下方式确保他将收到资金:
1. 检查发送账户是否有排队提现限额变化。
2. 检查发送账户余额是否足够高，不能过快清空。
3. 确保交易的优先级不低，并在网络中传播得足够多。

决定技术规格

迷你区块链

如果证明链提供了我们大部分的安全性，乍一看似乎几乎无需存储超过 1 或 2 个块的任何内容。当然至少需要有几百块，因为如果它太短，秘密链攻击就会变得更多可行的。我们至少需要一些合理数量的最小区块历史由出于多种原因，所有节点。我们认为 1 周对 Cryptonite 来说是一个不错的数字，但是在这个特定领域有很大的实验空间，可以找到最好的权衡。

我们需要考虑的另一个重要因素是块之间的时间。设置的太短可能会出现问题，例如由于块被隔离而导致更多的孤立块同时解决，但设置时间过长只会等待 1 次确认完全不切实际。基于对山寨币的简要检查，最佳出块时间似乎一般要在 1-2 分钟附近。 Cryptonite 的区块时间恰好为 1 分钟，因为它非常快但不是那么快，它会导致太多孤立块。

硬币供应和分配

比特币使用 2.1 千万个单位，其中每个硬币由 1 亿个单位组成，总共有 2100 万个硬币，可以被小数点后 8 位整除。然而，比特币内部使用 64 位整数，它可以处理更多的硬币，所以 2100 万听起来像是一个相当随意的数字，但实际上并非如此。许多应用广泛使用双精度浮点数，但双精度数只能存储整数 2^53，这就是比特币只有 2^50.9 个单位的最终原因。

但是，可以使用扩展精度浮点数来利用 64 位的全部范围整数。这使硬币供应具有更高的粒度级别，并且基于自然上限。具有 64 位粒度的硬币供应由大约 1844 亿个硬币，每一个都可以被 8 位小数整除。我们用过 Cryptonite 中的扩展精度浮动，因此我们不再受制于
双精度浮点数，可实现超大硬币供应。

可以通过多种方式分发硬币，使用 Cryptonite 需要 10 年时间一半的硬币供应被开采，重复半衰期为 10 年，但块奖励会在每个区块进行调整，以便随着时间的推移逐渐变化。突然的大变化在区块奖励中对网络不利，目前尚不清楚为什么比特币是旨在在区块奖励的变化之间有如此长的时间间隔。由于类似的原因，Cryptonite 也会更新每个区块的难度。

结论

在本文中，我们描述了比特币网络协议的一个变体，它被设计为消除对完整区块链的需求并显

着减少长期需求数据存储。这是通过将区块链的功能分离为单独的功能来实现的为执行某些任务而优化的机制。结果提供了一种纯粹的 P2P 加密货币，具有许多好处，例如增加了块空间。也有人建议，同态加密技术可用于实现高级别的隐私[11]。

帐户树和迷你区块链的性质也可能提供更高级别的用户隐私，因为旧交易可能无法定位，但我们不太可能没有节点专用于存储完整链。我们确实实现了更高水平的可扩展性一些安全权衡的代价，但没有什么不能处理的。最终结果确实具有高水平的安全性，但同时它超级紧凑且可扩展。在它在许多方面都优于比特币，但并非在所有领域（例如脚本功能）。

加密货币的未来会是什么样子？随着可扩展加密货币技术的出现，它看起来更好了。加密货币可以改变世界的方式可行，但前提是它的扩展性足以满足世界的需求。想法本身不是尽管如此，我们必须实施这些想法。从这个意义上说，中本聪是非常受人尊敬的因为他主动创建了一个极其复杂的系统，该系统建立在一系列新的和以前从未测试过的奇特概念，他永远改变了世界。

参考文献

[1] Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system.
http://bitcoin.org/bitcoin.pdf

[2] Blockchain.info. 2013. Blockchain Size Data.
https://blockchain.info/charts/blocks-size

[3] Andresen, G. 2013. Bitcoin-Qt / bitcoind version 0.8.0 released.
https://bitcointalk.org/index.php?topic=145184

[4] Reiner, A. 2012. Ultimate blockchain compression.
https://bitcointalk.org/index.php?topic=88208

[5] Todd, P. 2013. Bitcoin Blocksize Problem Video.
https://bitcointalk.org/index.php?topic=189792

[6] Bitcoin Wiki. 2013. Scalability.
https://en.bitcoin.it/wiki/Scalability

[7] Rosenfeld, M. 2012. Are there any studies into the size of the blockchain scaling over time?
http://bitcoin.stackexchange.com/questions/2798/

[8] Nakamoto, S. 2008. Re: Bitcoin P2P e-cash paper.
http://www.mail-archive.com/cryptography@metzdowd.com/msg09964.html

[9] Bruce, J. 2013. Cryptocurrency with Finite "Mini-Blockchain"
https://bitcointalk.org/index.php?topic=169311

[10] Mini-blockchain Project, 2014. Cryptonite. http://cryptonite.info/ and wiki: http://cryptonite.info/wiki/

[11] Franca, B.F. 2015. Homomorphic Mini-blockchain Scheme. http://cryptonite.info/files/HMBC.pdf