比特币的底层激励机制

支配比特币协议的经济暗流

Author	Aviv Zohar and Yonatan Sompolinsky
Translator	Taosheng Shi
WeChat Contact	data-lake
Mail Contact	tshshi@126.com
Organization	NOKIA
Document category	Distributed System
Document location	https://github.com/stone-note/articles

Version	Status	Date	Author	Description of changes
0.1	Draft	10/2/2018	Taosheng Shi	Initiate
0.2	Draft	DD-MM-YYYY	YourNameHere	TypeYourCommentsHere
1.0	Approved	DD-MM-YYYY	YourNameHere	TypeYourCommentsHere

Contents

1 引言

除了作为理财和转账的协议之外，比特币还创建了一个支配其内部运行的复杂经济激励机制(incentives)。这些激励机制强烈影响了协议的能力、安全保证，以及未来发展的道路。本文探讨了比特币协议的经济暗流、优势缺陷，以及它们如何反过来影响协议本身。

比特币，这个建立在开放 P2P（点对点）网络结构之上的货币（文献 9），继续享受人们的追捧。比特币系统是“无许可的”——任何人都可以选择加入网络，转账，甚至参与授权交易。比特币安全的关键之处在于它能够抵御攻击者以多重虚假身份加入系统的操纵行为。毕竟，任何人都可以下载比特币的源代码，成为一个比特币节点，并根据需要为网络添加尽可能多的计算机，而无需向其他人表明其身份。为了解决这个问题，该协议要求加入系统的节点展示出 “工作量证明”：付出算力破解密码学难题以获得参与比特币协议的资格。

从事这种“工作量证明”的节点被称为矿工。系统向矿工奖励比特币作为工作量的“证明”，从而也为这样的“算力投资”设定了“激励机制”。

通过在自己电脑上运行软件就可以获利（比特币）——这带来的第一个也是最明显的影响是：一旦比特币具有足够的价值，人们就开始大肆挖矿。事实上，为了增强挖矿力度，大部分挖矿工作很快都转移到专用的计算机农场。这些计算机农场使用定制工具来实现其目的：开始，GPU 被用于大规模并行工挖矿；之后，特需设计的芯片——专门针对比特币核心协议计算特征而量身定制的芯片——ASICs（专用集成电路）开始出现（在挖矿时， ASICs 机器比普通 PC 快一百万倍）。比特币网络迅速发展并变得更加安全，为了获利的竞争也变得更加激烈（利益由比特币协议周期性放出）。

比特币的安全性和经济性是相互作用的。在讨论这个主题之前，让我们快速回顾协议本身的规则——正是这些规则产生了这种复杂的相互作用。

2 1 比特币协议快速入门(A Quick Primer on the Bitcoin Protocol)

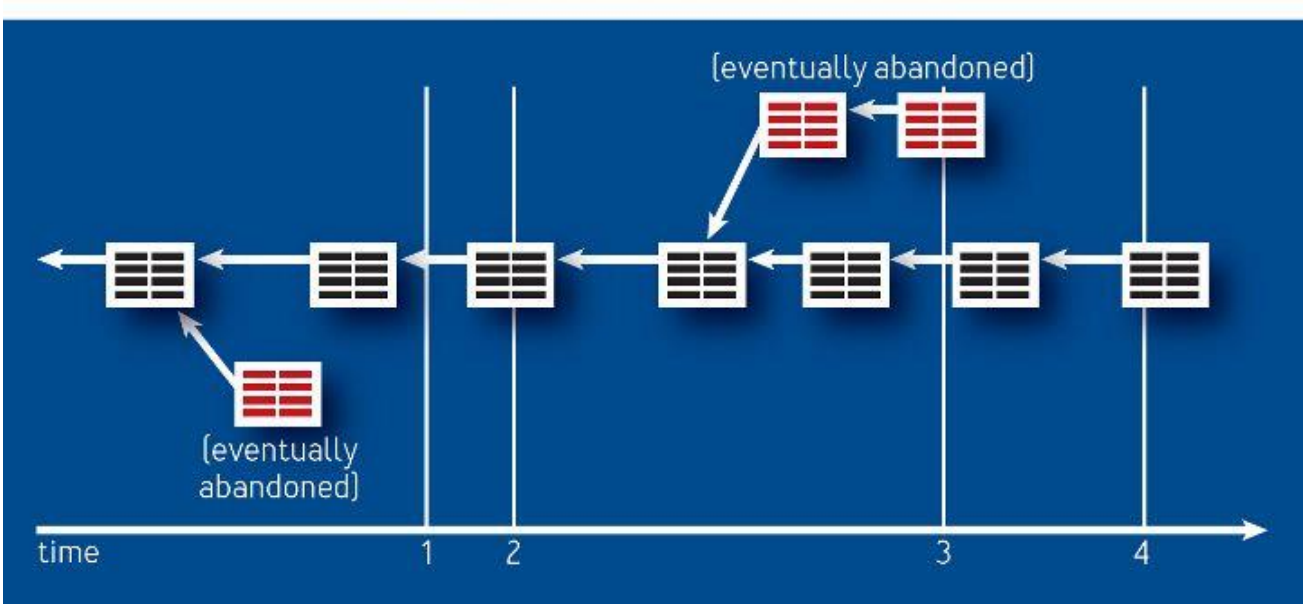
持有比特币并希望转账的用户可以将交易信息（通过他们安装在计算机或智能手机上的软件）发送到比特币网络上的一个节点。比特币网络中的活跃节点从用户那里收集这些交易信息并将它们分发到网络中的对等节点——分发方式是每个节点仅通知那些与请求转账所关联的节点。交易信息被批量的汇聚，称为区块，而区块又被链接在一起形成区块链，从而形成所有被接受的比特币交易记录。区块链中的每个区块都通过一个加密哈希值（实际上也是前驱区块的唯一标识符）引用其前驱区块。比特币网络中的每个节点都保存着完整的区块链副本。区块创建的过程被称为挖矿，挖矿的作用之一相当于新币的印刷，也就是所谓的造币。

比特币的协议规则使区块的创建非常困难：只有当区块包含密码学难题的答案时，才被认为是合法的。作为报酬，每当矿工成功创建区块时，他们都会得到比特币奖励。报酬由两部分组成：一部分是新造比特币，一部分是从区块所包含的交易中抽取的挖矿手续费。目前的造币率是 12.5 比特币每区块，这一数额大约每四年减半。随着这一数额的减少，比特币开始越来越依赖挖矿手续费来支付矿工。

因此比特币运行的关键是让所有节点就区块链的内容（区块链记录系统内的所有转账信息）达成一致。因此，区块更新会迅速传播到网络中的所有节点。不过，节点有时可能会收到两个不同版本的区块链。例如，如果两个节点同时创建了一个区块，则它们可能会持有区块链的两个不同更新（链的增长 chang）。这些区块可能包含不同的支付操作，因此比特币系统必须决定要接受哪个版本。

比特币协议规定每个节点只接受最长链作为交易事件的正确版本（主链），如图 1 所示（更确切地说，节点选择包含最多累积计算工作的链作为主链，这通常也是最长链）。这条著名的“最长链规则”为比特币提供了安全性。一个攻击者——如果试图愚弄其他节点，让他们相信系统发生了不同的支付事件——需要产生比网络其余部分更长的区块链。由于“工作量证明”是一个区块一个区块的创建出来的，“产生更长区块链”的任务将是异乎寻常的困难。事实上，只要攻击者的计算能力低于整个比特币网络的总和，区块链中的区块和交易将越来越难以取代（因为攻击者和整个比特币网络的链一起增长 chang）。

FIGURE 1: **THE EVOLUTION OF THE BLOCKCHAIN**



替换主链的困难性意味着攻击者需要多次尝试才能够偷天换日。这些失败的尝试意味着巨大的代价——在最长链之外挖矿，不会得到任何挖矿报酬。对于攻击者来说，初级的攻击确实代价昂贵（稍后将讨论更高级的攻击）。

图 1 展示区块链的演变情况：分叉开始出现，直到其中一个链比另一个链更长才能解决。解决的办法是丢弃最长链之外的区块：被丢弃的区块不再增长（chang）；其内容（红色部分）也被忽略；创建它们的矿工也不会得到任何报酬。在时间点 1，由于一个区块在创建时没有链接到最新的区块，导致产生两个可选的链，即发生了分叉。在时间点 2，分叉被解决，因为一个链比另一个链长。在时间点 3，有另一个持续时间更长的分叉，在时间点 4 第二个分叉被解决。

3 比特币经济学方法论：难度调整与挖矿经济均衡 (Bitcoin Economics 101: Difficulty Adjustment and the Economic Equilibrium of Mining)

根据比特币协议，区块创建速率大致保持不变，也就是期望区块的创建间隔大约为 10 分钟。如果块创建得太快，则生成区块所需的工作量证明的难度会自动增加。这种机制已经存在，以确保区块不会因为系统算力的增加而在节点之间“洪泛”。因此系统以相对恒定的速率向矿工提供报酬，和投资于挖矿的算力总量无关。

显然，随着比特币的价值上升（以美元计），挖矿生意（产生面值为比特币的支付）变得更加有利可图。随着更多的人为了利益加入矿工群体，区块的创建难度持续增加。而难度增加又导致挖矿代价变得更加昂贵。在理想情况下，当区块的创建成本等于所得的报酬时，系统将达到平衡。事实上，挖矿总是微利的，有风险的——而且还需要对设备进行初始投资，报酬中的一些盈余也必须补偿这些投资。因此，比特币协议的安全性可以根据价值调整自身：更高的价值也意味着更高的安全性。

由于挖矿报酬持续下降（根据比特币协议的挖矿时间表），预计创建区块的动机将更多依赖于交易费用。如果比特币交易量突然下降，这些交易费用将不足以补偿矿工的计算资源。一些矿工可能因此暂时停止他们的区块创建。这可能会危及整个系统，因为交易的安全性取决于所有诚实的矿工积极参与。（关于挖矿人数下降后的比特币激励机制，参见 Carlsten 等人的文献 3）

许多人抱怨说，创建区块的算力是在浪费资源（特别是电力）：为系统投入大笔费用，除了防范潜在攻击者之外，没有任何经济目标。工作量证明的确是在求解毫无用处的密码学难题——当然，除了为比特币网络安全保驾护航。但是，如果某些工作可能有用呢？或者可能以更高效的方式工作？如果挖矿不浪费每个节点的资源，那么攻击者也不会为攻击系统付出任何代价。事实上，如果工作量证明的成本较低，随着更多诚实参与者加入挖矿群体（获得报酬），难度调整机制将再次提高难度系数。因此，从某种意义上说，比特币的工作量证明机制就是为了“浪费”一定数量的资源，而不管个体矿工的效率如何。为了从挖矿中获得实质性收益而又不会因为成本的增加而抵消，就需要“工作量证明”——这对整个社会是有用的，但对个体矿工毫无价值。（更多使用其他难题作为工作量证明基础的尝试，参见 Ball 等人，Miller 等人和 Zhang 等人的文献：2,8,13）

4 挖矿的去中心化(Mining Decentralization)

比特币协议的关键是其去中心化：对于整个系统，没有单一的实体先验地具有比其他人更多的权威或控制。这增强了系统的抗毁能力：没有单一的信任锚点或单一故障点；矿工之间采用竞争的方式获得挖矿手续费。

为了保持这种去中心化，最重要的是要保证挖矿活动是由许多小型实体完成，并且没有一个矿工的算力明显超过其他矿工。理想情况下，给予矿工的报酬应反映他们投入的工作量：贡献了计算资源 α % 的矿工创建一个区块的 α %，并因此按比例抽取所有分配手续费和区块报酬的 α %。

在实践中，出于几个不同的原因，矿工可能从挖矿中获得不成比例的报酬。这种报酬分配的不平衡让利益偏向具有更多算力的大型矿工（使大型矿工获得比小型同行更多的利润），并为系统的中心化创造了持续不断的经济暗流。哪怕微弱的不平衡也可以危及系统：由于矿工可以使用额外回报来购买更多的算力，并因此而变得更加强大，继而提升挖矿的难度，最终将其他小型（因而利润较低）矿工排挤出这场游戏。由此产生的“赢家通吃”“动力学过程”将不可避免地导致系统的中心化，然后整个系统将受到优势矿工的支配，安全性也无法保证。

4.1 ASIC 挖矿(ASIC mining)

ASIC 的首次出现让比特币社区感到惊慌和担忧。在挖掘比特币方面，ASIC 的效率比以前的系统高几个数量级。最初，这种特殊的硬件并不容易获得，因此它为拥有者提供了比其他矿工更大的优势——以更低的成本挖矿。那些拥有这种优势的人为系统添加基于 ASIC 的工作量证明，直到难度级别高到其他人都放弃挖矿。当时的风险是：一个能够访问 ASIC 的大型矿工将最终主宰比特币系统。一段时间以后，随着 ASIC 的商业化并广泛分布，担忧逐渐消退。

事实上，ASIC 挖矿的实际影响（对安全性的贡献）是深远的。本文稍后将讨论矿工如何进行双重支付（双花）和私自挖矿攻击，以获取利益。然而，有人可能会争辩说，即使是自私和投机性的矿工也最好避免这种攻击。事实上，一位矿工投资数百万美元购买挖矿设备（比如 ASIC），相当于重金投资了比特币的未来价值：期望设备将在未来带来比特币回报。如果矿工使用这种设备攻击该系统，那么会降低人们对该货币的信心，并且降低比特币的价值和未来的回报。因此，矿工的利益在某种意义上与整个系统的健康保持一致。

总而言之，ASIC 挖矿提高了系统的准入门槛：普通人无法轻易地加入挖矿工作，也因此减少了系统的去中心化。另一方面，ASIC 挖矿也引入了一种退出的“门槛”：矿工无法将他们的设备用于其他经济活动，因此有助于提供系统的安全性。

加密货币（例如莱特币 Litecoin，本质上是比特币的克隆）之间出现的相互竞争——其中一些使用与比特币相同的工作量证明机制——为想要转移挖矿算力的矿工提供了选择方案。这让市场的“动力学过程”更为复杂。例如，当特定货币失去价值时，矿工会将挖矿算力转移到另一个加密货币，直到挖矿难度级别被提高。这可能会导致区块创建的波动，使矿工较少的加密货币系统变得不稳定。

4.2 非 ASIC 的挖矿系统(Alternative systems with no ASIC mining)

有趣的是，一些加密货币系统使用不同的难题求解（工作量证明）机制。这些难题难以设计成专用硬件，因而对 ASIC 挖矿更具抵抗性。例如，以太坊使用的 Ethash 难题。这通常是通过设计需要大量访问其他资源（例如内存等商用硬件）的算法难题来实现。

这些替代系统原则上更加去中心化，但另一方面它们缺乏“退出门槛”及其对安全的贡献。

当云挖矿服务变得高度可用时，也会产生类似去中心化的效果。一些实体通过云服务出租他们的挖矿设备。租赁云挖矿服务的客户才是真正的矿工，并且他们在系统中没有长期利益。随着这些云挖矿服务变得更加便宜和易于访问，任何人都可以轻松成为临时矿工。类似的是，云挖矿服务同样缺乏“退出门槛”及其对安全的贡献。

4.3 ASICBoost 算法(ASICBOOST)

回想一下，创建一个区块需要解决特定于该区块的密码学难题。这相当于猜测加密哈希函数的输入。求解这样的难题主要是通过强力枚举不同的输入来完成的。

矿工可以采用比同行更高效创建区块的方法来获得优势。除了采用更好的硬件外，算法是获得优势的主要形式。事实上，一个被 ASICBoost 的算法“trick”最近成为头条新闻。ASICBoost 使矿工能够重用一个输入猜测的算力到另外一个输入猜测。该算法是专有的，目前正在申请专利，尚不清楚谁可以用，谁不可以用。这样的算法带来的优势是可以降低每个哈希的算力消耗。ASIC 挖矿的大型制造商 Bitmain 最近被指控秘密部署 ASICBoost 的硬件变体以增加其利润。指控说，该公司在政治上阻碍了一些协议的改进，而这些改进很可能会让他们无法使用 ASICBoost。

4.4 通信基础设施(Communication)

另外一种提高矿工效率的方法是投资通信基础设施。通过更快地传播区块，并通过更快地接收其他区块，矿工可以减少其区块不属于最长链并被丢弃（“成为孤儿”）的机会。由于脱离主链的区块无法获得报酬，更好的网络通信意味着降低损失。无可否认，在比特币区块目前的创建速度下，这种优势微乎其微。 区块并不经常创建，并且交付加速几秒只能带来很小的优势。尽管如此，更好的网络通信是获得更多利润的一种相对便宜的方式。

此外，当比特币协议覆盖节点数增大并且交易处理加速时，通信优化带来的效果变得更加明显。目前比特币系统平均每秒处理三到七笔交易。改变比特币系统的参数——每秒处理更多的交易——将会增加孤儿区块的比率，并且会放大网络通信更好的矿工的优势。

4.5 规模经济(Economies of scale)

与任何大型实体一样，大型矿工可以享受规模经济效益。随着大规模挖矿业务的发展，大型矿工很可能投资于各种不同的优化方案，比如寻找成本更低的电力来源；或将挖矿设备放置在寒冷地区，为其设备提供更高效的冷却系统（挖矿带来大量电力消耗和机器冷却成为真正的挑战）。大型矿工也可以以更低的价格批量购买 ASIC 硬件设备。所有这些都转化为规模的自然优势——这种现象并非特定于比特币，而实际上出现在许多行业中。这些效应为大型矿工带来了优势，并慢慢地，将系统拉向中心化。

许多人担心，目前大部分比特币挖矿是由中国矿工完成的。与其他地区的挖矿相比，他们享有更好的 ASIC 访问，更便宜的电力和更低的监管。中国政府严格控制进出中国的互联网流量，并可能会破坏比特币系统，甚至没收境内的挖矿设备。

5 矿池和风险规避(Mining Pools and Risk Aversion)

比特币挖矿产生非常高的回报，但小矿工获得回报的可能性非常低。一个全时运行的 ASIC 设备挖掘到下一个区块的概率不到六十万分之一，这意味着几年内发现不了一个区块。这种高风险/高回报的收益并不适合大多数人。许多人会选择较长时期的小规模固定收入（这实质上是风险规避，文献 6）。例如，可以使用固定收入来支付挖矿的电费。

5.1 矿池的形成(The formation of pools)

矿池是矿工联盟。联盟将矿工的计算资源整合在一起，挖矿报酬在成员之间共享。由于矿池比每个矿工单打独斗挖掘到的区块要多得多，联盟能够更经常地向每个矿工支付小额的报酬。

从比特币网络的角度来看，矿池也只是一个挖矿节点。矿池成员与矿池服务器交互，矿池服务器将正在处理的下一个区块头发送给所有成员。每个成员都试图求解相应区块的密码学难题（事实上，他们使用同一个区块的变体，并且工量证明也略有不同，以避免重复工作）。每当成员找到一个区块的难题答案时，就会将该区块发送给矿池管理节点，管理节点又将该区块发布到比特币网络。该区块向矿池提供报酬，管理节点随后将报酬分配给矿池中的所有成员（扣除一部分小额费用）。

5.2 矿池报酬分配和篡改可能(Reward distribution within pools and possible manipulations)

大多数矿池是公开矿池，并向任何有意愿参与的人开放。显然，矿池必须采取措施，确保只有真正贡献算力的成员才能享受相应的回报。为此，每个矿池成员发送部分难题求解答案（工作量证明）给矿池—— 这些部分答案“接近”成为区块的完整难题求解答案。部分答案比完整答案更加普遍，而且任何求解这个难题的成员都可以提供持续稳定的算力（低于目标）。这可以表明成员确实在工作，并且可以评估每个成员能够贡献的算力。因此，矿池按照份额数量占比支付成员报酬（每份提交的部分难题求解答案都会获得一定份额）。

幸运的是，找到难题求解答案的矿池成员无法窃取报酬。密码学难题取决于区块头，该区块头由矿池的管理员控制。密码学难题对区块本身的内容（通过加密哈希）进行编码，包括区块报酬的接收者。在找到特定区块头的难题求解答案之后，除非使难题求解答案失效，否则不能篡改区块头。

尽管如此，矿池还是可能被策略矿工的篡改。

跳池(Pool hopping)。在比特币的早期阶段，矿池分局每个矿工提交的部分难题求解答案数量的份额，简单地将所有矿工挖掘的最新块的报酬按比例分配给所有矿工。份额数量是通过对同一个池创建的前一区块进行测量得到的。

一些矿工提出了一种提高报酬的方法：如果一个矿池运气不好，并且一段时间没有挖到区块，那么很多部分难题求解答案（份额）就会积累起来。如果矿池发现一个区块，它的报酬将被分成许多小份。产生额外的份额的工作量与以前一样，但由于这个原因产生更低的预期回报。相反，矿工可以跳到最近找到一个区块的另一个矿池，并且每个额外的份额都会获得更高的预期回报。如果这种行为被大量采用，那么实际上，暂时不成功的矿池会被所有理性的矿工完全抛弃。对抗跳池的报酬计划很快被开发出来，并被大多数矿池所采用（文献 10）。

区块发布抑制攻击(Block-withholding attacks)。虽然矿工无法窃取难题求解答案的区块报酬，但他/她仍然可以否决对矿池中其他矿工的报酬。矿工可以选择只向矿池管理者提交部分难题求解答案，但放弃所有成功的难题求解答案。因此，当其他人找到难题求解答案时，矿工会收到一定比例的奖励，但不会为该矿池提供任何实际贡献。抛弃成功的难题求解答案破坏了矿池，攻击者仅损失少量的收入作为代价。

尽管攻击者蒙受了损失，但在某些情况下，矿池有必要利用自己的一些挖矿能力破坏竞争对手：攻击矿池通过将其中一些矿工注册为受害矿池中的工人，渗透到受害矿池中。这些工人然后执行区块发布抑制攻击。通过成本和报酬的详细计算，表明在某些情况下（取决于攻击矿池和受害矿池的大小），攻击矿池是有利可图的（文献 4）。为了防止这种攻击，人们已经提出了对挖矿协议的轻微修改。在

修改后的版本中，矿工无法辨别部分难题求解答案和完整难题求解答案，以解决工作量证明问题，并且无法选择性地抑制完整的难题求解答案。

5.3 消除矿池(Eliminating pools)

虽然矿池适合小型矿工，可以减少矿工的风险和不确定性，但矿池会给系统引入一些中心化。矿池管理员本质上是大量矿工的整合计算资源的控制者，因此权力非常大。一些研究人员提出挖矿协议的技术修改方案，彻底破坏公共矿池的存在（文献 7）。在该方案下，在找到区块有效的难题求解答案后，挖掘该区块的矿池成员仍然可以将报酬重定向到自己（而不会使难题求解答案失效）。假设大量矿工会为自己申请报酬，那么矿池将不会有利可图，因此会解散。

6 攻击和违反规则的经济学原理(The Economics of Attacks and Deviations from the Rules)

本文前面描述了一种矿工在比特币协议中取得支配地位的方法——既可以获利超过他/她应得的份额，也可以在链中产生更多的区块。迄今为止讨论的方法没有违反协议的任何规则；从某种意义上说，允许矿工充分利用他们的硬件和基础设施。本节讨论直接违反协议规则的行为——矿工谋取自身利益以牺牲他人利益为代价。从某种意义上说，这种策略的存在意味着协议的激励结构中存在根本性的缺陷：为了利润最大化的理性参与者不会遵循比特币协议。

非正式地，协议规定任何节点：（1）验证它接收的每个新消息（区块/交易）；（2）将所有有效消息传播给其对等节点；（3）新区块一旦创建立即广播出去；（4）在节点本地已知的最长链上构建新区块。对协议的攻击对应于这些规定中的一个或多个偏差/违反。

6.1 校验(Validation)

不校验传入消息的矿工是脆弱的——下一个区块可能包含他/她未校验的无效交易，或无效的前驱块引用。其他节点会认为这个新区块是无效的并忽略它。这明确地激励矿工在他们的区块中只嵌入有效的交易并在接受之前校验每个新区块。

有趣的是，尽管有这样的逻辑，但有时矿工会在一个区块之上挖掘，而没有完全校验该区块。这种做法被称为 SPV 挖矿（SPV：simplified payment verification，代表简化的支付校验，通常指使用不读取区块完整内容的瘦客户端）。

为什么矿工会在未经校验的区块上创建新区块？答案还是在于激励机制。甚至在接收到区块全部内容之前，一些矿工采用这样的方法来得到新创建区块的哈希 ID（一种称为间谍挖矿 spy-mining 的方法：加入另一个矿池来检测区块创建事件）。即使接收到一个区块，校验其包含的交易也需要时间。在此期间，矿工意识到区块链已经长了一个区块。因此，为了避免挖矿设备在该区块校验完成之前（极有可能是有效的）处于闲置状态，矿工决定在该区块之上继续挖矿， 为了避免下一个区块与未验证区块的交易冲突的风险，矿工不会在下一个块中嵌入新的交易，以期仍然能够收集区块的报酬。

确实有证据表明有矿工正在采取这种方法。首先，被挖掘的区块中有一小部分是空的（即使许多交易正在等待批准）。另一个证据与 2015 年 7 月发生的一起不幸事件有关。一个无效区块（无意）由于

bug 而被挖掘，SPV 矿工在其上增加了五块额外的块，而未做校验。当然，其他校验矿工拒绝该区块和任何引用它的区块，导致网络中有六块长的分叉。在分叉中丢弃的区块可能包含双重支出的交易。

这个事件显示了 SPV 挖矿的危险之处：SPV 挖矿降低了比特币的安全性，并可能在区块链中引发分叉。幸运的是，矿工大大提高了区块的传播和校验时间，所以 SPV 挖矿效果越来越差。空置区块奖励的下降（计划中）也会降低矿工参与此类行为的动机。

6.2 交易传播(Transaction propagation)

比特币协议的第二个重要方面与信息传播有关：新的交易和区块应发送给网络中所有对等节点。这里对遵守协议规定的激励并不那么清楚。矿工甚至可能会抑制发送尚未被纳入区块的未确认交易，特别是交易费用较高的交易（文献 1）。矿工有很强的动力来保持这种交易，直到他们成功创建一个区块。向他人发送交易允许他们抢先获得交易提供的报酬。迄今为止，大多数交易费用相对较低，而且没有证据表明高手续费交易以这种方式被扣留。

接下来，让我们把注意力转到有意操纵区块链的协议违反/偏差上。

6.3 私自挖矿(Selfish mining)

每当矿工创建一个新区块时，比特币协议表示新区块应该在矿工观察到的最长链条的顶部（即，最长链的顶端为前驱），并且矿工应该立即将新区块发送给网络中的对等节点。

不幸的是，矿工可以通过违反这些规则并有策略的行动而受益（文献 5,11）。矿工的总体策略是不发布区块并私自延伸公共链作为其私链。同时，公共链也被其他（诚实）节点延伸。策略矿工只有在其私链长度不能胜出的概率较低时才发布其私链。当策略矿工这样做时，所有节点都采用矿工突然释放的较长的链，如协议所规定的那样，并且他们放弃了以前的公共链。

重要的是，这种行为增加了矿工在最长链中的份额——也就是说，它增加了最终产生的最长链上的区块的百分比。回想一下，比特币系统会自动调整工作量证明的难度，以保持区块的创建速率不变。因此，从长远来看，在区块链中占有相对较大的块数比例意味着矿工绝对报酬的增加。

没有准确的办法来验证矿工是否从事私自挖矿。鉴于只有极少数区块是孤立的，似乎私自挖矿还没有被孤立区块采纳，至少没有被大型矿工采纳（能够从私自挖矿中获利最多的矿工）。一种解释是，长期尝试这种操纵的矿工可能会损失他们的声誉并引起社区的愤慨。另一种解释是，这种方案需要在最初失去一些自己的区块，并且只有长期运行才能盈利（协议重新调整难度级别大约需要两周）。

6.4 双重支出(Double spending)

双重支出是对比特币用户的基本攻击：攻击者向网络发布合法支付，等待它嵌入区块链并让受害者确认，然后发布更长的私自挖掘区块链不包含这笔款项。这笔款项不再是最长链条的一部分，就像“从未发生过”。

这种攻击会带来一定的风险：如果攻击者的区块不能成为最长链的尾部，则可能失去对他/她的数据块的报酬。令人惊讶，而且不幸的是，持久的攻击者可以通过遵循更复杂的攻击方案来消除这种风险（文献 12）。这些方案通过频繁的放弃攻击，发布私有的攻击链，并为它的区块收集报酬。通过在

每次失去报酬的风险过高时重置攻击，攻击者可以弥补攻击成本，甚至长期盈利。这些方案本质上是私自挖矿和双重支出攻击的组合。

目前，网络中的双重支出并不常见。这可能是因为成功执行的双重支出是非常困难的，或者因为能够成功执行此类攻击的矿工也对系统声誉拥有重大利益。

7 结论(Conclusion)

激励机制确实在比特币协议中发挥着重要作用。激励机制对于比特币协议的安全性、及其日常运行的有效性至关重要。正如本文所指出的，矿工为了最大限度地增加收入而费尽心机，并且经常会找到一些创造性的方法，而这些方法与比特币协议并不符合。

加密货币的协议应该建立在更加坚实的激励基础之上。还有很多领域需要改进，包括基本的挖矿报酬机制，交互共识机制，矿池的报酬分配机制，以及交易手续费市场本身的方方面面。

8 作者简介

Dr. Aviv Zohar is a faculty member at the School of Computer Science and Engineering at the Hebrew University of Jerusalem, and a cofounder and chief scientist of QED-it. He has been researching the scalability, security, and underlying incentives of cryptocurrencies for several years.

Yonatan Sompolinsky is a Ph.D. student (final year) at the School of Computer Science and Engineering at the Hebrew University of Jerusalem, under the supervision of Dr. Aviv Zohar. He obtained an M.Sc. in computer science and a B.Sc. in mathematics from the Hebrew University. He is cofounder and chief scientist of DAGlabs.

9 参考文献(References)

1. Babaioff, M., et al. 2012. On Bitcoin and Red Balloons. Proceedings of the 13th ACM Conference on Electronic Commerce: 56-73.

2. Ball, M., et al. 2017. Proofs of Useful Work. IACR Cryptology ePrint Archive: 203.

3. Carlsten, M., et al. 2016. On the Instability of Bitcoin Without the Block Reward. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security: 154-167.

4. Eyal, I. 2015. The Miner's Dilemma. IEEE Symposium on Security and Privacy.

5. Eyal, I., Sirer, E. G. 2014. Majority is not Enough: Bitcoin Mining is Vulnerable. International Conference on Financial Cryptography and Data Security. Springer Berlin.

6. Fisch, B. A., Pass, R., Shelat, A. 2017. Socially Optimal Mining Pools. arXiv preprint.

7. Miller, A., et al. 2015. Nonoutsourceable Scratch-off Puzzles to Discourage Bitcoin Mining Coalitions. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.

8. Miller, A., et al. 2014. Permacoin: Repurposing Bitcoin Work for Data Preservation. IEEE Symposium on Security and Privacy.

9. Nakamoto, S. 2008. Bitcoin: A Peer-to-peer Electronic Cash System. Bitcoin.org; https://bitcoin.org/bitcoin.pdf.

10. Rosenfeld, M. 2011. Analysis of Bitcoin Pooled Mining Reward Systems. arXiv preprint.

11. Sapirshtein, A., Sompolinsky, Y., Zohar, A. 2016. Optimal Selfish Mining Strategies in Bitcoin. International Conference on Financial Cryptography and Data Security. Springer Berlin.

12. Sompolinsky, Y., Zohar, A. 2017. Bitcoin's Security Model Revisited. International Joint Conference on Artificial Intelligence, Workshop on A.I. in Security. Melbourne.

13. Zhang, F., et al. 2017. REM: Resource-Efficient Mining for Blockchains. Cryptology ePrint Archive. https://eprint.iacr.org/2017/179.