区块链论文阅读

“Proof-of-Work” Proves Not to Work version 0.2

在我们 AI 课程中，我们学习了利用贝叶斯分布来判别垃圾邮件，效率很高质量也很不错，但这只是解决了垃圾邮件的“查阅”(被拦截的邮件大部分不会被查阅)，并没有从根源上解决垃圾邮件的输出，这篇文章就是关于这样一个问题：怎么减少垃圾邮件的发送，Dwork 和 Naor 提出让每一个邮件发送者进行一个复杂计算,作为证据证明这个邮件值得被接受,本文则表明这个方法并不靠谱。

阅读介绍的同时我也一直在思考什么样的方法会阻止一个人发垃圾邮件呢？首先他发的原因可能有：1，好玩，我不能排除这种情况，有些人也许就是喜欢发一些垃圾捉弄别人。2,有利可图,我们收到的垃圾邮件大部分都是广告邮件，发邮件不收费，而且可以批量群发，这种宣传方式简直是 0 成本。本文提出“工作证明”付出成本的方法不可靠，阅读到这里，我之前并没有考虑到工作证明还可以用到垃圾邮件判断上，所以根据介绍我想到了现有的垃圾邮件的一些问题，于是类比这种机制提出我自己的设计：

假设每个账号都有一个账户并且有足够的余额，同时有一个基础信用值，发一封邮件需要 1 人民币，发过去后先按照过滤算法分类，如果邮件被接收方查看，且为被用户标记为垃圾邮件，则 1 元退回原账户，如果查看后发现是垃圾邮件如果用户标记为垃圾邮件，则这 1 元转入到接收者账户里，发送方的信用值则被减 1，那 1 元也回不去了。还有一种情况就是不是垃圾邮件但是收件人长期未查看（比如闲置邮箱，或者登录了邮箱却故意忽视那些未查看的邮件），则限定一个时间比如最近有登录但是一个月内这个邮件没有被查看则 1 元则退回原账户（没被查看信息也就没产生价值他的目的也没达到），如果是一年内没登陆（自然没被查看）那么扣费 0.1（或者 0.5 元等归邮件公司），但是不扣信用值。这样

也有一些问题，比如A向B发了邮件，但是并不知道B已弃用了那个邮箱，他的正常邮件就会被扣费，相比作恶的人有些无辜，但是由于我们实在无法判断所以只能一起收费了，还有就是可以通过我是否被扣费来判断我的邮件是否被已读，我们有些时候并不想让对方知道邮件是否已阅，这涉及到隐私，我们或许可以设置已阅返金一个月后再退回账目，这样如果发送者收到退款就无法判断是对方看到不回还是一个月对方没有登陆了。这样有个好处就是发送邮件人发送前考虑到自己是恶搞或者垃圾邮件有可能会被扣信用值和扣费而放弃发送，而那些很诚实的人也不必担心损失因为他们的邮件被查看不会被标记为垃圾邮件或者长期未读发送金也会被退回他们也没什么损失，如果是长达一年未阅的也仅仅扣费0.1元其余返回损失也不大。但是类比垃圾短信，即便是收费我们还是能收到大量的垃圾短信，因为作恶虽然相比免费多了成本，但是比起获利成本真的是微不足道，所以设置一个高昂的发送金利用接收者判断是否是垃圾邮件，如果判断是垃圾邮件发送金还会归入接收者这样他们做标记工作也就不是“白做”的了，当然还要考虑是否有人故意把别人的邮件设置为垃圾邮件而收取发送金获利，如果发送的人确实靠谱，他如果乱标记那么他也许就下次会收不到这个人的邮件了，错过一些信息也是有代价的，或者可以建立一个记录，如果一个人标记的垃圾邮件数目很多或者很多别人标记为正常邮件的他却大量标记为垃圾邮件，那么这个人很有可能有问题，就可以考虑收回他的收费资格。

回到论文中，第二部分先简要回顾了一下“工作证明”系统：

发送方生成一个字符串，其密码哈希以一定数量的零开始，生成的字符串的关键部分是电子邮件收件人地址，时间戳和唯一值或“ nonce”，该值会反复变化，直到所需的零数为在加密哈希值中找到。它的特点是验证很简单但是破解代价非常高，同时有个问题就是非常浪费电力，因为这些计算都没什么用，还有个问题就是算力集中偏离了区块链开始的去中心化的特点，除此之外用户的机器计算能力有差别也需要考虑。

第三部分是对工作证明的定量分析。

分别估算了电子邮件数量,邮件列表分布情况(假设电子邮件是均匀分布的,则平均每天约60个合法的非列表电子邮件由每个主机发送),每个工作证明设置成本为C。

第四部分是用户发送邮件需要做多少的计算。这里提到了很多的问题和因素,比如成本利润等的计算对C的影响,邮件服务器的存在,垃圾邮件发送者接管的机器等等。

第五部分提出速率限制对合法用户带来的影响。

第六部分做了总结:两种限制方法都阻止不了垃圾邮件发送,因为关于高利润产品的垃圾邮件依旧具有经济意义——他可能获取的利润可能远远高于发送的成本。限制发送数量的方法也不可行,因为他们可以窃取受攻击的计算机来帮助他们发送邮件。还可以利用白名单通讯录(减少好人的工作证明工作量),同时“坏人”依旧需要做工作证明。但文章最后表明:除非垃圾邮件发送者的成功基础能够显著增加,并且不安全的最终用户机器数量大幅度减少,否则不可能有效(我之前自己的设计没能考虑到这点)。

Majority Is Not Enough:
Bitcoin Mining Is Vulnerable

我们都知道,比特币是一个基于点对点网络的去中心化数字货币系统,应用区块链完成交易的记录,使用工作量证明机制和最长链规则作为共识机制,使各个节点比特币的账本达到一致性。比特币系统先天可以遭受51%攻击:当某个节点拥有全网50%以上算力的时候,其从理论上可以实现账本的篡改,从而实现所谓的双重花费攻击。而51%也就成为比特币系统的安全阈值了。

然而，我们也需要思考一下比特币系统的安全阈值真的为50%吗？是否有其它可能让比特币系统的安全阈值降低到50%以下？答案是肯定的。这篇论文就提出了一种实现方法叫作自私挖矿攻击，文中证明，理论上此种攻击可以将比特币系统的安全阈值从50%降低到33%。

给出了一种在挖矿之外，可以获得更大收益的算法，同时这个算法不利于整个网络的利益，证明了比特币POW不是激励相容的。

一般人们认为比特币的POW是激励相容的(incentive-compatible)，即大家都单纯地追求自己的利益最大化，按照这种方式去做，同时能够达到全局的最优结果（安全性高，TPS高等）。

激励相容：

在市场经济中，每个理性经济人都会有自利的一面，其个人行为会按自利的规则行为行动；如果能有一种制度安排，使行为人追求个人利益的行为，正好与企业实现集体价值最大化的目标相吻合，这一制度安排，就是“激励相容”

第二部分：比特币，区块链和矿工机制的介绍。

第三部分：自私挖矿

这篇文章中提出的算法称为自私挖矿,核心思想就是，私自矿池挖出新块之后，暂时不发布这个区块（私下保存）,让其余的网络算力浪费资源去挖掘 ，然后自己继续挖下一区块，当发现网络上别人也挖出新区块时再发布这个区块，可以获得更高的收益。

同时这个更高收益的算法并不是全局最优的，因为矿工会为了更高的利益进行自私挖矿，使得自私矿池越来越大，逐渐变成多数，破坏了比特币的去中心化。虽然在自私挖矿攻击中，诚实和自私矿池都会浪费算力，但是诚实矿池浪费的算力会更多，同时自私矿池可以获得比自己诚实挖矿更高的收益. 此消彼长，矿工会更愿意加入自私挖矿。而且，自私矿池的算力越大，它能够获得的奖励高于线性增长. 这更加有利于自私矿池吸引更多矿工加入。

过程：

1，自私矿池挖到块 A 之后不直接发布全网， 只在自己的矿池中广播该块，形成私有链，并且继续挖下一块 B。

2，当检测到网络上有人发出下一块 A'时， 再广播自己挖到的块， 使网络进入竞争状态.

3，如果自私矿池挖出 B 时，直接发布，让全网转到自己的链上，自己获得块 A 和块 B 的收益，同时浪费掉了网络在 A'以及分叉上使用的算力。

4，如果诚实节点在块 A 后挖出了新块，那么自私矿池享受块 A 的利益。

5，如果诚实节点在块 A'后挖出新块，那么自私矿池不获利。

第四部分：分析了奖励系统并得出收益公式：

$$R_{\text{pool}}=\frac{r_{\text{pool}}}{r_{\text{pool}}+r_{\text{others}}}=\frac{\alpha(1-\alpha)^2(4\alpha+\gamma(1-2\alpha))-\alpha^3}{1-\alpha(1+(2-\alpha)\alpha)}.$$

并做了模拟验证得出结论：使用自私挖矿将使池获得比其相对规模更大的收入。因此，其矿工将获得比其相对采矿能力更多的收入。因此会有更多的理性的矿工加入自私矿池以获得更大的收益。

第六部分：提出加强协议的方法：对协议进行简单的更改，如果所有非自私的矿工都采用 γ，则将 γ 设置为，因此将的阈值设置为向后兼容：矿工的任何子集都可以采用它而不会妨碍协议。 而且，它是渐进式的：采用它的矿工的任何比率都会降低 γ，因此会增加阈值。

第七部分：关于以下几点的讨论：

1，系统崩溃比特币协议被明确设计为去中心化的。

2，检测自私挖矿有两个自私挖矿的网络特征码可以用来检测何时发生自私挖矿，但都不容易确定地进行测量。

3，措施与对策

4，自私的采矿给比特币生态系统带来两种危险：自私的矿工获得不成比例的回报，而动态则有利于自私的矿池向多数增长，从而产生雪球效应。

5，负责任的披露由于比特币的去中心化性质，自私的采矿只能受到集体，共同行动的阻碍。

最后做了总结：

比特币是第一种广泛使用的加密货币，拥有广泛的用户基础和丰富的生态系统，所有这些都依赖于激励措施来维持关键的比特币区块链。 同时模拟结果表明，比特币的挖矿协议与激励机制不兼容。 文章介绍了自私挖矿，这是一种采矿策略，可以使共谋的矿工池采用该策略，以赚取超出其采矿能力的收入。 更高的收入可能导致新的矿工加入自私的矿工池，这是一种危险的动态，使自私的矿池可以发展为多数。 如果采用可以阻止自私矿工的自动化机制，则比特币系统将更加强大。 作者同时对比特币提供了向后兼容的修改，以确保小于总采矿能力 1/4 的矿池不能从自私的采矿中获利。 最后表明，至少有 2/3 的网络需要诚实，以阻止自私的采矿，而不仅仅是 51%就可以了。