zencash

修改中本聪共识
防御51%算力攻击的提案
区块递交延迟的惩罚机制

2018年6月14日

Alberto Garoffolo, Pier Stabilini, Robert Viglione, and Uri Stav

介绍

最长链法则（又称中本聪共识）在 2009 年推出时运行良好，因为当时的算力环境较为去中心化。此后，算力资源越来越趋于集中，而算力租赁成本也降低了，因此原先主导性的策略（即根据规则来参与挖矿）对于所有秉持最长链法则的工作量证明（PoW）区块链来说不再适用。最近发生的一些事情也证明了，在某些情况下对正在运行的公链网络发动 51% 算力攻击从经济角度来说是可行的。本白皮书提议对中本聪共识进行创新性调整，使得针对任何基于工作量证明的挖矿加密货币系统发动此类攻击的成本变得极度高昂，因此降低其可能性。

发动双花攻击的常见方法如下：

- 执行交易 T_1，将地址 A 中的币发送至现有公链上的交易所地址
- 在包含交易 T_2 的平行分叉链上私下挖掘一个区块，这个交易将币从地址 A 发送至另一个地址
- 等待 T_1 被交易所完成确认，在此期间继续私下挖掘平行链，挖掘速度比公链更快
- 在交易所上卖出经确认的币，随后提现至私人地址 B
- 向全网广播这一长于公链的私链
- 在此时，全网将会把攻击者的私链视为新的公链（因为它更长），矿工将在这一刚经调整的公链上开始挖矿
- T_1 不再被视为有效交易，但攻击者已经将相关的币通过欺诈的方式花出去了

总而言之，这些攻击是可能发生的，因为系统允许在用户接受特定交易后（例如，在交易所等待确认时间之后）使用新的区块链来“覆盖”区块链历史记录的当前节点视图。这遵守了中本聪在比特币白皮书中给出的原则，并且为大多数 PoW 加密货币投入实施。PoW 共识中的区块生成是一个随机过程，诚实的矿工可以在相同的高度上并行生成区块（概率取决于区块生成时间和网络延迟），中本聪共识有一个简单的方法来判断 – 即是最终默认采用积累最多工作量的链。 因此，摈弃具有累积较少工作量的较短分支已成为令横跨多个分布式系统的区块得到有序排列的有效方式。

中本聪的白皮书基于这样一个假设：即大多数算力被诚实节点所控制（“一个 CPU 一票” 原则）并且在这个假设之下，几乎不可能创建任何合理长度的敌对分支来实现双花攻击。传统的探索式算法一致认可：仅需等待区块完成几个确认之后，交易遭到取消的概率就非常低了。

自比特币白皮书发布以来，许多事情发生了变化。危害最长链法则的一些重大变化是 ASIC 矿工和其他算力提升技术的出现，这些技术彻底打破了“一个 CPU 一票”的原则。 许多加密货币具有相同的挖矿算法，但算力却存在着极大的差异，这导致某一加密货币的矿池算力有可能被用于攻击另一个链。

因此，我们发现在当下的环境中，中本聪的“大多数算力是诚实的、以及较长的敌对分支不可能出现”这个假设被打破了，近期发生的针对几个加密货币的 51% 算力攻击就证明了这一点。我们需要一个更先进、更全面的系统来满足现时情况。核心的 PoW 共识需要得到修正，以提供安全的服务，同时仍应允许诚实矿工生成冲突区块以及合理的网络延迟同步。

为了实现这一目标，我们定位并确定了一项改动。这一改动将大幅提高发动双花攻击得以成功而所需要的资源（对诚实算力没有影响），并将攻击成本在经济上变得完全不再有利可图。此外，攻击得以成功所需的资源的提高并不需要接收方（包括交易所）增加确认数。

区块递交延迟的惩罚方法

考虑到私下挖矿是双花攻击的源头，为了使其不那么凑效，我们引入了一个惩罚措施，来针对区块接受延迟（相对于该区块隐藏起来而不被公共网络发现的时长）。时间以区块间隔数为单位进行测量，而不是通过时间戳这一时间维度进行测量。

举个例子，让我们假设现有如下这一区块接收场景：
NB_i = 普通区块
MB_i = 恶意区块

NB100 - NB101 - NB102 - NB103 - NB104 - [...] - NB116 - NB117 - NB118 - NB119 - NB120

MB100
MB101
MB102
[...]
MB119 - MB120 - MB121 - MB122

时间轴 ——————————————————→

图示 1

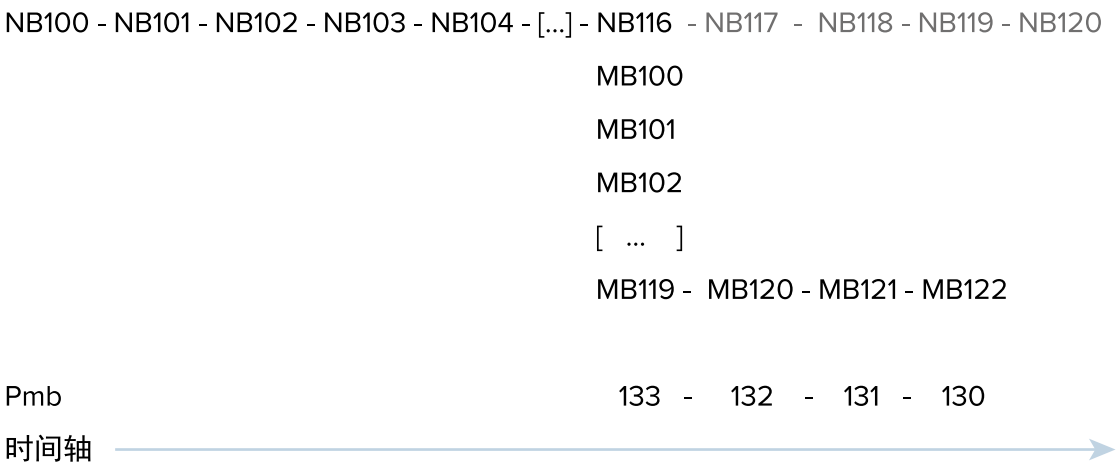
在当前机制下，区块 NB117、NB118、NB119 和 NB120 将不会被挖出来，因为全网在接收到区块 MB119 之后，恶意链将成为活跃链；全网将废弃原先的正常链，从区块 MB119 开始在恶意链上挖矿。

为了防止这种情况发生，我们引入了一个与分叉链从公共网络上隐藏时长相对应的分叉接受延迟的概念。这一延迟代表了在新的平行链被采用前需要得到的被推迟的区块数量。对于攻击者而言，这意味着即使在恶意分叉链被发现后，他还是需要继续在分叉链上挖掘，直到延迟完成为止。

举个例子，让我们考虑如下的延迟函数 *DF*。为了定义 *DF*，我们首先引入 *BDi*，其有效地表示区块接收延迟，定义为当前主链高度和接收区块的高度之差（例如 BDmb100 = 16，BDmb101 = 15，...，BDmb115 = 1，BDmb116 = 0，BDmb117 = −1，BDmb118 = −1）或 −1（在接收区块的高度大于当前主链高度的情况下）。

在这种情况下，整个分叉链的延迟函数 *DF* 将代表 BDmb［i］值的总和，其中 i 表示分叉链中区块的编号。

在图示 2 的下列例子中，延迟 DF（MB100,...,MB119）= 16+15+14+13+12+....1+0−1−1−1 = 136 − 3 = 133 个区块。所以攻击者将需要在公开他的分叉链之后继续挖掘额外的 133 个区块，这样分叉链才能被其它节点所接受。



图示 2

在使用这样一个延迟函数的情况下，举个例子，如果我们假设采用 20 个区块的确认时间，那么 21 个区块的延迟惩罚将会是 21 *（21 + 1）/ 2 = 231，那么为了实施攻击所需要挖掘的最小区块数量将是 231 + 21 = 252 个。

请注意，只有在分叉开展后，确认时间才能开始计算。

对这一延迟函数进行适当调整会使得攻击复杂到难以实现，因为它将需要极大的算力资源，并且在分叉最终能被采用之前给予了更多的时间机会做出反应。全网将会得知这一争议分叉，并将在全网默认该链为真实可用之前不得不减少完整的延迟函数（*DF* = 0）。在此期间，全网参与者（譬如交易所）可以冻结潜在的欺诈存款，直到问题获得解决；例如，要么废弃试图进行欺诈的链，要么通过粗暴直接的方式成功地将 *DF* →0。诚实矿工可以继续在活跃的可用链上挖矿。

为了保护低算力的币种，这个延迟函数同时也考虑了当前的挖矿难度（*d*）（比如，依靠一个和当前难度成反比的系数来增大这个延迟）。这样对于 $DF' = DF * f(d)$ 的增大因素在设置 $f(d) = 1$ 的情况下可以被忽略，但任何合理的函数形式都可以替代，只要它对诚实的并发区块的竞争范围影响很小，然后可以在超出合理范围之外成倍地延展，进行指数级延展，以应对不诚实的动机行为。

尽管该引入特性使得挖矿攻击（通过挖掘私人平行分叉来执行）的整体威胁变得复杂，但它并不妨碍全网在自然分裂的情况下进行汇合（例如，当全网的某些部分与其它部分完全隔离开一段时间后）。达成汇合的周期将比纯粹的最长链法则来得长，但诚实矿工将通过令 $DF \rightarrow 0$ 来汇合多条链。

请注意，如果攻击者公开挖掘他的链，那么这一延迟就不再适用，但在这种情况下每个人都会发现分叉链，并且能够采取预防性措施（譬如，交易所将会增加确认周期等）。

结论

加密货币系统的运行环境与 2009 年诞生之初相比，发生了重大变化，当时挖矿算力要比现在去中心化得多。中本聪共识（又称最长链法则）简单地将具有累积最大工作量的链视为自然的链分叉，在这一机制下运作得很好。技术上的限制和经济上的激励相结合，使得最长链法则成为了任何矿工（无论是诚实的还是邪恶的）的主导策略。但现在情况已经不再如此，公链需要更新共识法则，令发动双花攻击得以成功的成本比当下要变得高昂很多。

本提案给出了这样一种方法：就本身而言，前景是相当乐观的。其形式简单，但是可以用延展函数进行概括，令试图发动双花在技术上不可行、经济上损失重大。这一方法能够公平对待同时算出区块的诚实矿工，并且公平对待（后续得到解决的）合理的网络延迟。任何攻击媒介都不应该被轻视对待，或认作就此完全失去效果，但这种方法肯定会使其中一种常见的攻击手段的成功可能性变得极小。对分层防御策略的进一步研究，例如在该惩罚机制之上引入间隔区块公证方案，可以使该机制更加安全，因此会在适当时候进行调查研究。

作者

Alberto Garoffolo, Pier Stabilini, Robert Viglione, and Uri Stav

致谢

特别感谢

为此文献做出贡献的团队和社区成员:

@cronic, Peter Stewart, @ultimateblockage,
Rosario Pabst, Rowan Stone, Gustavo Fialho and Vitalik Demin.

创意设计： Lucy Wang, Linda Baksija and Marko Orčić.

翻译：俞振翰