

读书笔记 3: On Availability for Blockchain-Based Systems

文章对区块链的可用性进行了探讨并对于交易信息没有被提交以及提交时间影响因素进行了研究，同时制定了优化的终止机制。

全文从以下几个因素对交易记录没有被提交以及提交时间太长的影响进行了调查：网络排序、用户定义的 **gas price**、**gas limit**、**block gas limit**；并且按照比特币和以太坊各自的特点进行了详细的分析：

(1) 在对于比特币的交易提交中：作者首先交代了重组对于提交时间影响的重要作用，同时提到交易手续费作为激励机制也是一个不可或缺的影响因素，接而介绍了“孤儿”的定义，也提到 **locktime** 这个因素以及造成无序到达的原因。在进行这一部分的实验中，文章介绍了它的数据采集方法：通过两次实验，每次持续约 25 小时，收集进入池中的比特币交易，同时确定区块链中提交的时间，在这些交易事务中，分为直接接受、被拒绝和孤儿三种交易事务，而对于重复的日志，文章也采用了一定的机制进行滤除与检查。从实验中总结出：无序到达对于提交时间的影响确实很大，但是较低的手续费并不是孤儿提交时间延长的原因，而 **locktime** 对于孤儿提交时间的影响作者认为不能称之为决定性因素。

(2) 而在以太坊的交易提交中：文章首先介绍了以太坊的工作周期，也看出与比特币的不同之处，它从公告到被包含进区块到包含到链，仍然有风险无法最终确认。而对于这方面提交时间因素的影响，作者也介绍了它的数据收集方法：通过修改客户端节点来监听收集事务，同时将最低 **gas price** 定为 0，客户端连接设置可以达到 500 个节点，而对于交易也会记录当地的时间，同时做了一定的数据误差剔除机制。实验总结出：每笔交易随着被包含次数的增加，它的延迟时间会越来越长，即越是需要更多的区块去确认一笔交易，就越需要花费更多的时间；而用户定义的 **gas price** 影响上，一开始随着它的上升，提交时间会加快，但是当到达一个门限值 25 后，几乎没有什么影响了；而对于 **gas limit** 则没能发现什么强相关的影响；同时在排除了 **gas price** 的影响下，网络延迟导致的无序性进而严重影响了提交时间的增加。

(3) 在对于以太坊的 **block gas limit 的研究中，**文章说明了这样的限制是为了防止 DDos 的攻击，但是当限制在刚好一些关键点的时候，会严重影响到一些合同无法部署而导致许多交易无法完成。

(4) 对于优化的交易终止机制上，文章提出了两种方式：可以通过发起接收为自己的竞争交易，也就是具有相同随机数的另一个交易来像是终止上一笔交易；也可以通过重试发出交易来使得相应的其他事务过时而无效；而文章也对三种情况进行了实验：交易没有在常规时间包含进区块、客户端想收回交易、费用不足而无限等待，均取得很好地交易成功效果。

感想：

- (1) 这篇文章让我对区块链有了一定的了解，同时对于比特币以及以太坊它们的一些情况有了更加深入的认识，也了解到它们存在的一个很棘手的提交问题，对于它们的影响因素也是有了一个入门级的了解。
- (2) 我对于这个问题的理解主要是同步问题，由于同步的问题使得交易的无序性变得严重，进而导致提交时间以及提交交易的一系列问题。
- (3) 自己之前也没想到区块链存在着这么一个提交不确定性的问题，也觉得一些必要的机制需要建立。

改进方案:

- (1) 从更多的角度来研究影响提交时间的因素，甚至是它们的组合影响而不仅仅是单个因素的影响，根据缩短提交时间的因素进行优化
- (2) 对于同步和网络延迟的问题，确实需要合适的机制来合理缓解这一块的压力。