

以太坊很慢——极其缓慢。

最近做一个简单的USDC审批交易，大概花了3个小时进行验证。

这里有一个更有启发性的统计数据：以太坊平均每10~20秒发布一个区块。每个区块包含少于350个交易。所有这些大致转换为每秒30个交易。

当批评以太坊的缓慢时，Visa的2000 tps经常被提起。也许这是一个不公平的比较，因为以太坊仍处于开发阶段。

然而，以太坊似乎不太可能在短期内主宰数字金融。

以太坊的低吞吐量是一个基础性问题。

以太坊是一个基于账户的区块链：账本状态被定义为一个从账户地址到一段数据的键值映射。

简单的ETH交易(价值转移)可以实现账户对ETH余额数据的增减。同样，更复杂的交易(合约调用)将改变指定帐户的数据。

在这种情况下，以太坊交易是全球账本状态的转换函数。这就是让以太坊虚拟机(EVM)图灵完成并允许智能合约成为可能的原因；以太坊智能合约本质上是一个可交互的账户数据。

现在让我们看看EVM如何处理或验证这些交易。并行处理所有交易是不合理的。按照设计，所有交易都试图改变整个全局状态。

如果交易并行运行，EVM将偏向于竞态条件：两个程序(在本例中是交易)尝试并行地增加uint变量。因为两个程序同时访问变量，所以变量只增加一次而不是两次。

为了解决此类并发bug，以太坊选择逐个处理交易。换句话说，EVM是一个单线程状态机。

因此，以太坊实现了Concurrency（并发），而不是Parallelism（并行）。

以太坊类似于只有一个出纳员的票务队列，其处理时间不一致。排队的人是等待验证的交易，唯一的出纳员是虚拟机。当我们考虑到gas费用时，事情就变得更加复杂了。现在，任何人都可以额外付费插队。超长的队伍意味着那些不能花钱买到更

好位置的人将不得不等待过多的时间来处理他们的票。

以太坊的低吞吐量是个问题，尤其是从web3.0的角度来看。以太坊确实成为了所有web应用程序的媒介。如果它目前的吞吐量持续下去，像为Reddit上的一篇帖子加赞这样微不足道的任务可能需要超过两个小时的时间来处理。我们生活在一个速度决定一切的时代，以太坊太慢了。

可能会问，为什么不选择性地应用并发性呢？

更详细地说，为什么不将并发应用到冲突的交易上——例如，将价值转移到同一个帐户上——并并行处理其余的交易。不幸的是，Saraph和Herlihy已经向我们表明，所实现的加速充其量是适度的。

已经提出了许多加速以太坊并提高其可扩展性的解决方案。最近的EIP-1559——伦敦硬分叉——并不直接影响以太坊的交易速度，但理论上应该通过减少普通用户在交易处理前必须等待的潜在区块数量来稳定其在大规模交易峰值上的波动。然后是L2的rollup，这应该会直接影响以太坊的吞吐量，而不会破坏区块链宝贵的去信任。

与此同时，其他模拟通用虚拟机的区块链也在积极开发中。有些已经成功实现了并行，承诺吞吐量远高于以太坊的30 tps。特别关注Algorand、Solana和Cardano，以及他们在智能合约中实现并行化的独特方法。

上述就是区块链智能合约中的并发性和并行性的详细内容，更多关于智能合约中的并发性和并行性的资料请关注（www.dadaqq.com）Dadaqq.Com其它相关文章！

本站提醒：投资有风险，入市须谨慎，本内容不作为投资理财建议。

Tag：区块链 智能合约 并发性 并行性