对 PoS 的简单技术批评

> 这是我在 2020 年 10 月 28 日上海上海以太坊社区聚会 Eth2 圆桌上的发言，比较了 PoW 和 PoS 在纯粹技术层面的区别。总结起来说，PoS 就是比 PoW 更差的抗女巫机制（在区块链场景下），因为（1）在区块链这样的分布式系统中，带宽是最稀缺的资源，而 PoS 的带宽开销更大；（2）从节点个体来考虑，资源无非花在验证共识和验证区块上；给定去中心化要求（节点的硬件条件不变），把资源花在前者上面一定导致能够花在后者上面的资源减少，而 PoS 的共识验证开销更大，所以其可扩展性一定更差；（3）PoW 的共识验证成本不会随着 PoW 生产者的增加而增加，但 PoS 的共识验证成本会，所以出块权的去中心化跟网络的安全性反而起了冲突。
>
> 这三点在现实中皆有实际例子可以验证。
>
> 但在场的 Vitalik 仅以缺失性比较（Eth2 客户端的运行负担比 Eth1 的小）硬件来敷衍（当然更小，因为当时的 Eth2 客户端根本不处理以太坊网络上的交易，等于是拿 Eth2 的共识跟 Eth1 的交易验证相比）。
>
> 全文可见此处：https://mp.weixin.qq.com/s/rWKgcaHC-PmBz8815RecYw。

我想去挑战Vitalik，他认为PoS有很多优点，相对于它的牺牲是值得的。我在这里的挑战是：在我看来，这件事情不像我们想象的那样可持续，根本原因在于两个点：

（1）PoW的这个世界中，生产工作量证明的过程和节点间的P2P通信过程是分开的。也就是说你可以有无数个矿工在网络之外，随便在哪里，生产PoW证明，其实你不会占用这个系统内部的带宽开销。但是PoS刚好相反，要生产证明必须要在系统内部不断与其他验证者通信来产生终局性，会占用系统内部的带宽开销。在我看来，这是技术上的非常大的不同。

（2）其次在于验证，如果你只是要验证这条链的共识，在PoW里面非常简单，你只需要验证工作量证明即可，而在PoS世界中，它对于共识的验证，必须要验证每一位共识参与者的签名是否有效。假设有128位参与者，就需要验证128个签名，即使采用BLS的签名方案，可以通过聚合减少数据开销，但不能节约验证的次数，仍然要验证128次。

我觉得可以得出一个结论在于，PoS系统的验证者的增加会导致内部开销和带宽成本上升，这是非常大的缺点，而在PoW中并不会出现这样的情况。这只是共识层，而没有涉及交易。如果我们把验证者的开销分为验证共识的开销和执行交易的开销，PoW可以保证第一部分的成本长期保持在比较低的水平，但PoS第一步的成本会随着共识的参与者数量的增加而不断增加。这在我看来是非常大的缺陷，这使我不太相信PoS系统可以做到长期的发展，这个是我在这里比较核心的观点，就是这个属性让我觉得PoW可以在长期发展中保持相当好的竞争，因为它的节点在共识层的开销是相当低的。注意是验证共识而非参与共识。