## **1. POW在安全性上的困局**

POW的项目，其安全性正比于其上挖矿的算力。但是在任意时刻，或者一小段时间内，世界范围内能用于挖矿的算力是相对固定的（假设都是通用算力）。因此各个不同的区块链项目对算力的争夺是存量竞争，这就像是个切蛋糕游戏，你切的多一点，我就切的少一点。而可怕的是，切的少的项目就变得不安全，就有被流动性算力（被购买，或者从大项目竞争失败的算力）攻击的风险。而且面临着浪费能源等的指责，所以新项目很少见到用POW共识的了。

## **2. POW的价值**

但是我认为POW与POS相比，还是很有其价值的，因为POW是一种”客观“证明，而POS是一种主观证明。比如POW上当你想分叉，或者双花时，你就是要实实在在的付出那么多算力，这需要拥有对应的矿机，并且花费对应的电能。POS是一种主观证明，它靠的要么是验证者用抵押的币做背书，或者自己的身份做背书（POA)，来直接对区块进行签名就行了，这里的成本是抵押的币或者是身份信用，但这个成本的验证就很复杂和可变了。节点可以零成本在同一个高度对多个不同区块进行签名。区块链的安全性在POS里，取决于诚实节点占的比例。这就很主观了，或者说，不那么可靠。

## **3. POW共识的改进方案**

### **3.1 方案**

因此如果能够有一种方法，让各个项目在POW上不再是存量竞争，而是合作，那就既可以解决POW项目的安全性，又能同时保障共识的客观性。下面提出一个想法。

区块链目前正在朝着模块化发展，模块化包括代码的模块化和资源的模块化。我们可以考虑把算力和共识，从多个项目中抽取出来，组成一个共享的算力池，通过算力池挖矿，来同时保护用到该池的项目。具体方法如下：

各条链独立打包自己的块，计算自己的“状态”，在新块出来后，可以把交易根、状态根等需要共识的内容发送给算力池。在算力池中，会收到多条不同链的交易根（仅考虑交易共识），可以把这些不同链的交易根生成一个merkle树，针对该树根挖矿。挖矿完成后，各条链可以各自将挖矿所得的nonce，状态根，以及相关的SPV证明打包，完成新区块。

### **3.2 效果**

无论有多少条链使用该算力池，算力池提供的算力保护都是同样的，不会因为链的加入而降低。该方案相当于把算力模块化了。

* 对于链来说，可以获取更高的安全性。
* 对矿工来说，可能以同样的成本获取多条链的币。

因此该方案应该是有吸引力的。比较理想的结果是不同项目共同维护同一个算力池，比较差的结果是出现多个算力池来竞争获取算力，这就又变成切蛋糕问题了。

## **4. 补充**

4.1 各条链的出块时间需要同步吗？

不需要，新的交易根生成后，直接发送给算力池即可，算力池可以随时更新用于挖矿的merkle树根，新交易根的加入不会影响挖矿时间和效率

4.2 该方案其实是受 [王嘉平](https://www.zhihu.com/people/04fc21702d9cd64ce06dfe13a7d35d90" \t "https://zhuanlan.zhihu.com/p/_blank)先生的monoxide的启发而来的，其实是monoxide的一个简单扩展。