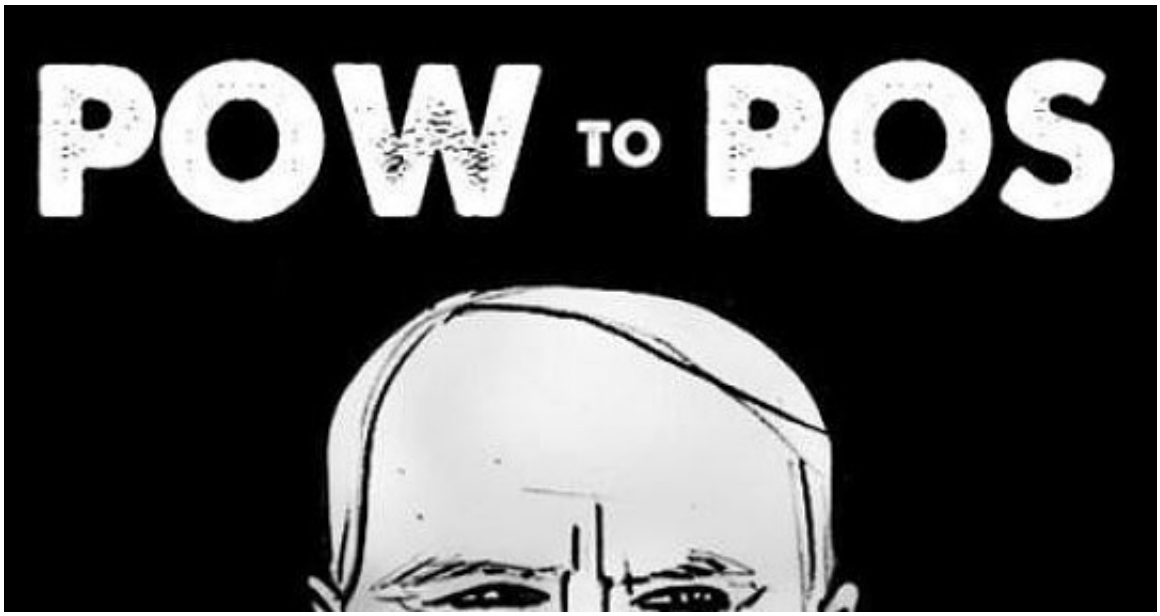
区块链领域的安全问题一直是大家讨论的焦点，Peter 认为在设计一个较为安全的系统之前，首先要明确一下安全的定义，本文给出的是我自己的观点。我学术背景是电气自动化工程，职业背景是程序员，所以观点肯定是技术世界观的。根据这里给出的安全定义，能够解释我为何是一个 POW 的支持者，另外为何对某些 POS 项目表示怀疑。安全的定义我自己的安全的定义是防守能量和攻击能量比值。下面来解释一下。

首先，安全是一个能量问题。城墙修的再厚，如果有足够的炮火，一样可以把它打烂。这里防守能量是修筑城墙的能量，花的能量越多，城墙就能修的越高越厚。攻击能量是炮弹中保存的能量。另外一个例子，如果你理解密码学的话，就知道世界上没有不能破解的密码，只是因为很多密码的破解需要花费攻击者难以负担的能量消耗，所以才有被认为的暂时安全的密码存在。




第二，安全是一个比值。工程上有个概念叫做安全系数，安全系数足够高，我们就认为系统是安全的。具体来讲，安全系数指的是安全程度的系数，是极限应力和许用应力的比值。举个简单的例子，一个载人的升降机，绳子的极限承受能力是10000千克，工程上一般载人的许用总重量就是1000千克，安全系数是10。这里，防守能量是绳子的粒子之间的引力，这个能量可以保证绳子不断。攻击能量是人身体带来的重力。

第三，攻击收益为负的系统就认为是安全的。安全是一个相对概念，工程上认为，如果绳子用来载人，那么安全系数要达到10，而如果运输货物，安全系数为5就足够了。一个普通铁柜子，保存我的私人物品就认为是安全了，但是如果是保存一堆黄金，就不够安全。原理还是可以套用安全是个比值的这个思路，攻击潜在获利多，那么认为攻击能量就很大，所以防守能量也必须提高，才能保证安全。

总结一下，安全是一个能量比值，攻击收益为负的系统，就认为是安全的。

世界上能否共存多个 POW 系统?

基于之前的安全定义，我自己是支持用 POW
去保证系统安全的。同时我也认为，这个世界上可以有多个 POW
的区块链同时存在。

POW 的安全来自攻防能量对比。最著名的 POW 系统肯定是比特币了。比特币会以最长链作为最终的共识结果，矿工向哪个分叉上添加区块就相当于支持这条分叉成为最长链。这是用区块来进行投票的过程，而生成每一个区块都是有能量损耗的。这样，攻击者要攻击比特币网络，也一样要花费能量，51%攻击意味者，攻击者的能量水平高于全网其他诚实节点的能量之和的时候，攻击就会成功。结合咱们之前所说的，安全是攻击能量和防守能量对抗的思路，可以看出比特币的 POW
机制是完全符合本文对安全的定义的。所以说，POW
的能耗不是白费，它的回报是安全。

另外一点，咱们的 Andreas
说过，可能我们这个世界只能负担的起一个POW系统。

我自己一开始也是这么认为，觉得什么事情都应该在比特币上做，不要另外再开新的 POW 的链。但是实际上，往比特币上堆太多功能会降低比特币的安全。于是大家还是启动了不少 POW
的链。以本文的逻辑推导，这个是可以接受的，理由如下。如果世界上只有一条 POW 的区块链，也就是比特币，那么比特币承载的价值就是全世界，那么要用全世界电力的50%以上去保护她，因为一旦攻击成功的收益就是全世界。但是，如果另外有一条 POW 链，承载了一部分价值，此时比特币承载的价值低了，那么对应的电力当然也可以分给另外的链一些。比特币不再承载全世界，意味着攻击收益就低了，对应攻击能量也会低，所以减少一些防守能量不会影响比特币的安全。

总结这部分，POW 用能耗换来安全，不能算是浪费。建设多条 POW
链，不会降价任何一条的安全。

POS 到底安全吗?

下面从反面来论述一下我的观点。POS 是一种类似股东投票的共识机制，特点是不需要耗费能量。从前面的论述可以推论，POS
肯定是值得研究的，但是不耗费能量的机制注定和安全无关。

首先展开聊一下为何 POS 不能保证安全。POS 系统为安全支出的能量为0，意味着防守能量为0，那么不管攻击能量是多少，安全都为0。POS 系统往往都设计的非常复杂，原因就是作恶是无利害的，投票既然没有成本，攻击者就可以为了自己利益的最大化去随意投票了，在此基础上去设置各种审查和惩罚也是治标不治本的。

POS 的现实意义应该是有的，可以依托信任或者 POW 系统的安全来构建完整系统。但是， POS 本身不提供安全，POS 系统运行必须找到自己的安全基石。目前很多链把 POS 本身作为安全基石，然后在上面构建各种功能，个人认为这个思路是值得商榷的。

结论：区块链系统是复杂的，改变一个预置条件，可能结论就变了，所以我也会保留修改本文结论的权力。写作本文的目的是跟各位做一下思路上的沟通，希望我的思考过程能够有启发性。