21 ETH 权益证明

挖矿最大的问题就是太费电。以太坊平均每个交易的能耗是67度电，而比特币每个交易是1000度电。主要是因为以太坊的出块时间比较短，所以平均到每个交易的花费就是比较少的。

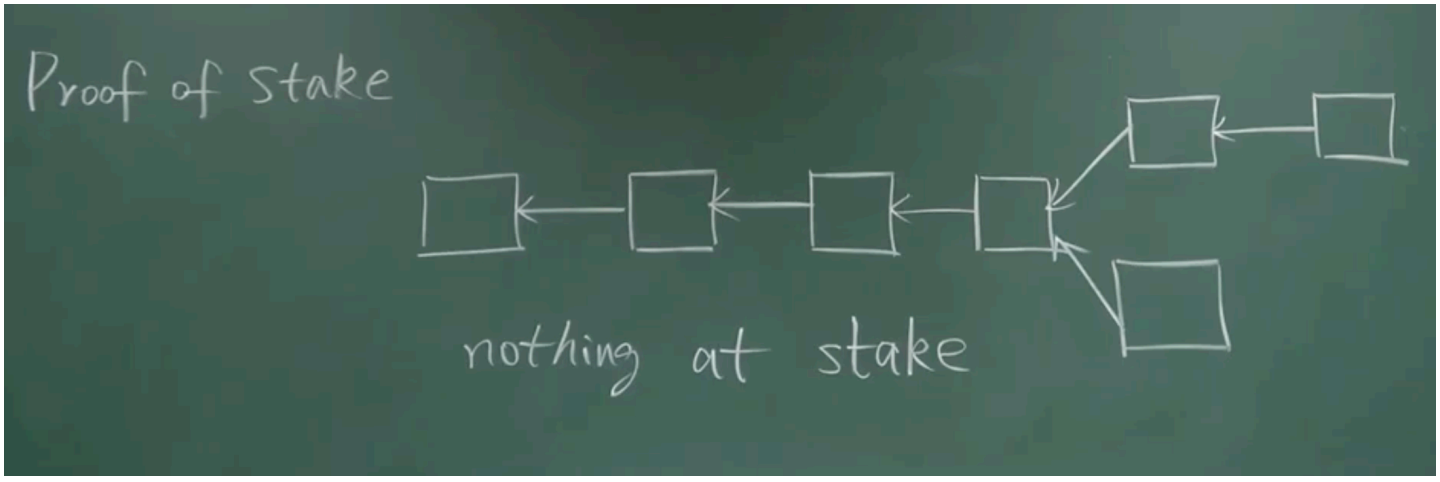
权益证明的基本思想：
因为比特币和以太坊中获得收益的多少是由挖矿来决定的，而挖矿是由算力决定的，而算力是由具体有多少设备来决定的，而设备是有投入多少钱来决定的。那我们为什么不直接把钱掏出来比钱就完事了？现在的做法是大家都拿钱去买矿机，然后通过算力来竞争。我们可不可以直接大家按照投入的钱的多少来决定？比如说我出一百万，你出五十万，那么我的期望收益就是你的二倍。这就是权益证明的核心思想。也有的时候管这种思想叫做virtual mining。采用virtual mining的加密货币，一般会预留一部分作为pre-mining和pre-sale。

proof by work的矿机是由区块链社区外部的法币来购买的。现在虚拟货币的总市值和股票市值根本没办法比。所以想要发动攻击，比如说我在股票市场上很有钱，我就可以购买大量的矿机来进行攻击。尤其是对于一些处于早期的货币，这种攻击是致命性的。AltCoin，infanticide扼杀在摇篮里。但如果改成权益证明，就是闭环的了。因为是按照币的持有量来投票的，如果想发动攻击，必须买入半数以上的币。这个时候就会导致币的价格反而大涨，对于开发者来说未必是坏事。有点儿类似于股份制公司招收恶意收购。

proof by work和proof by stake是不互斥的，可以混合。比如说持有币的数量越多的话，这个矿工挖矿的难度就越低。但是这样的问题在于持有币数量最多的矿工挖矿一定是最简单的。所以很多加密货币采用了proof by deposit的方式，就是你可以投入一定的币用来降低挖矿的难度，挖到矿了之后这些币就进入CD了，需要冷却一段时间，等之后才能再次用。

权益证明的挑战：

1. 两边下注（nothing at stake）：
   我就把钱分散的给两条链（因为都有可能成为最长合法链），即使最后没能成为最长合法链也没有关系，反正我下注的钱只是放在这里（并不影响后续花，只是没有收益而已）。



以太坊中采用的权益证明共识机制是casper the friendly finality gadget(FFG)，在过度的阶段也需要和proof by work混合使用。

要想成为一个validator，必须投入一定的保证金。validator的作用就是促进系统达成一致。validator投票的权重取决于保证金的大小。这个时候还是有人挖矿的，挖100个区块作为一个epoch。这个类似于数据库里面的two-phase commit。Prepare message， Commit message。每一轮投票的时候，需要得到2/3以上的validator同意。

实际上epoch只有50个区块，每一个epoch只需要进行一轮投票，这个投票会作为上一个epoch的commit message以及下一个epoch的prepare message。必须两轮投票都得到2/3以上的多数，才能奏效。

验证者参与这个过程的好处就是可以得到一些奖励。而如果验证者不作为，或者乱作为，被发现了会扣除或者销毁全部的保证金。每个验证者会有任期，任期到了会开始冷却，这个时候别人可以检举验证者。如果通过了，才可以取回当初的保证金和奖励。

那通过validator投票的finality（最终交易）能否被推翻呢？如果一个恶意组织，仅仅是矿工的话，永远没办法攻击成功。必须是有validator同伙，而且必须有1/3以上的validator是两边都下注的。这样他们的保证金就都没了。

权益证明不是很成熟，而工作量证明经过时间检验是非常成熟的。有一个新币叫柚子EOS，采用的是完全的权益证明，用的是叫DPOS的协议。Delegated Proof of Stake。选21个超级节点。

电很难存储和传输。而挖矿提供了一个手段，可以把电转换成加密货币。而加密货币是非常好传输和保存的。所以挖矿反而可以消耗过生产的电，带动经济。