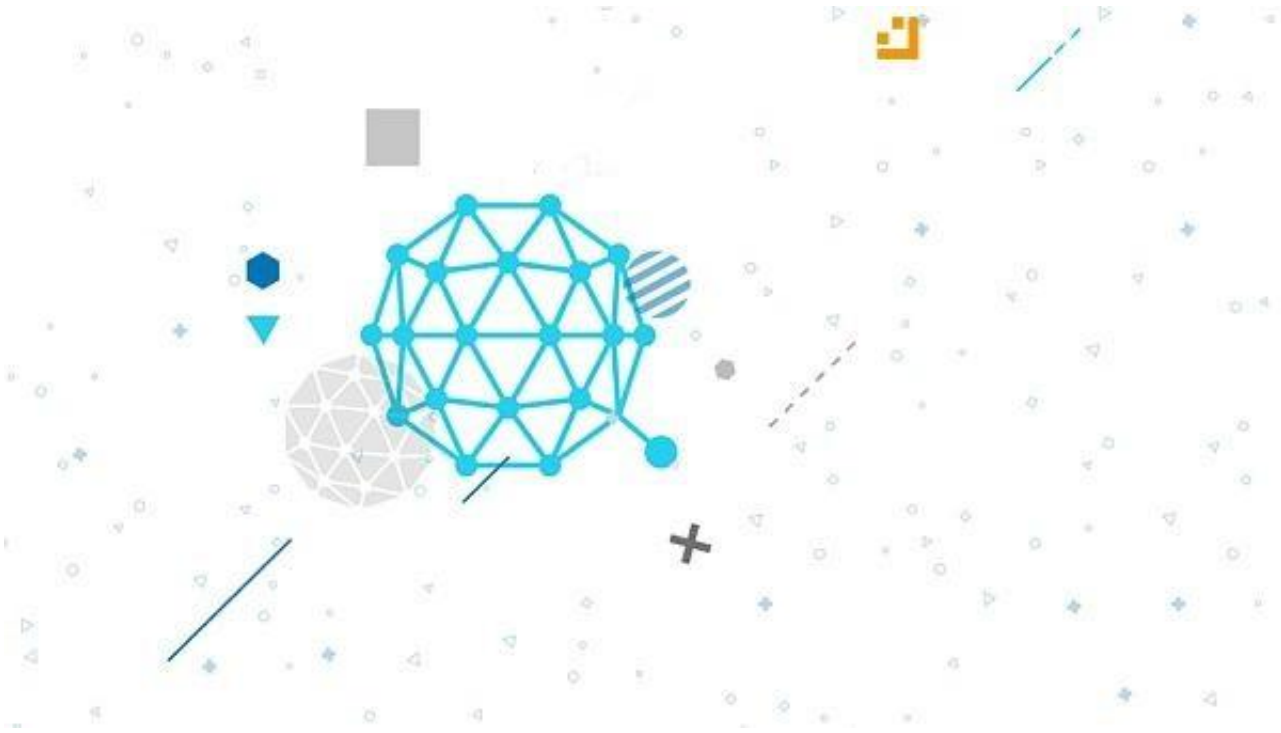
在浅谈区块链(二十二)我们谈到权益证明，而关于区块链的权益证明，闻西又有了新的认识，在此分享给大家。

1）权益证明也叫股份证明机制，核心就是谁持有币越多，谁就越有可能挖到矿。

它就类似于财产储存在银行，这种模式会根据你持有数字货币的量和时间，分配给你相应的利息。

简单来说，就是一个根据你持有货币的量和时间，给你发利息的一个制度，在股权证明POS模式下，有一个名词叫币龄，每个币每天产生1币龄，比如你持有100个币，总共持有了30天，那么，此时你的币龄就为3000，这个时候，如果你发现了一个POS区块，你的币龄就会被清空为0。你每被清空365币龄，你将会从区块中获得0.05个币的利息(假定利息可理解为年利率5%)，那么在这个案例中，利息 = 3000 * 5% / 365 = 0.41个币，这下就很有意思了，持币有利息。



2）权益证明有点类似于资本主义。

即谁拥有的币多，且持有的时间越长(即币龄越大)，谁就越有话语权，你挖矿所能得到的奖励也就越多。

3）权益证明发起51%攻击的可能性非常微小。

因为想要进行51%攻击的话，你得拥有51%的货币。也就是说，这东西越值钱，攻击的成本就越高。

简单的来说，你都拥有51%的钱了，你还发起攻击干嘛，这就有点像：如果你在某家公司拥有51%的股份，你已经是最大的股东了，还发起攻击干嘛？

而比特币的工作量证明机制，是因为你持有的是算力，最终目标是通过算力来获取“货币”，即需要对算力进行转化的，而权益证明不需要转化(因为你已经直接持有了“货币”了)，所以工作量证明发起51%攻击的意义比权益证明更大，可能性也更大。