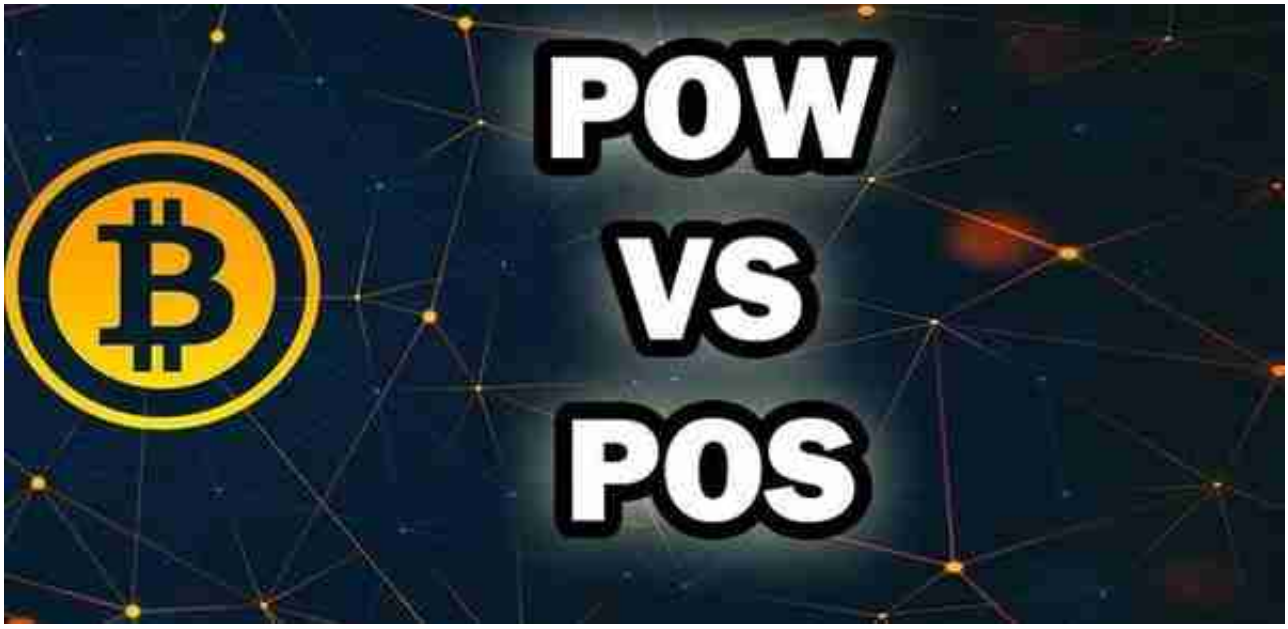
本文重点：区块链经常出现的POW、POS、DAG、DAC这些缩写是什么意思呢？想知道就仔细阅读本文

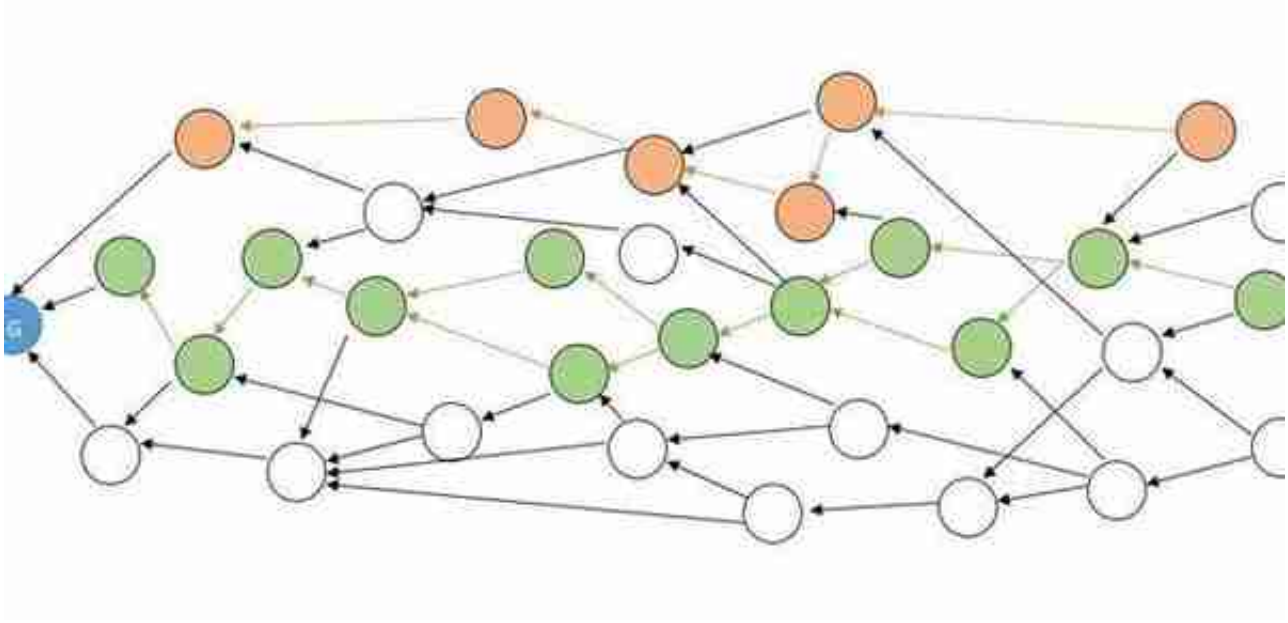
区块链经常出现的POW、POS、DAG、DAC是什么呢？

PoW+PoS



- POS：全称 Proof of Stake，股权证明。 这又是什么意思呢？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(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，非常好！（需要注意的是，5%的年利率仅仅 是举例，并非每个 POS 模式的币种都是 5%）

什么是DAG？



区别于大家熟知的比特币采用的为链式结构，DAG 的解决方案是，将最长链共识改成最重链共识。传统区块链设计上，新单元的发布会加入在原先的最长链之上，并且所有节点 认为最长链为真，依次无限蔓延。而 DAG
中，每个新加入的单元，不仅仅只加入长链里的 一个区块，而是加入到之前的所有区块。假设当你发布新交易时，前面有两个有效区块，那
么你的区块会主动同时链接到前面两个之中，DAG
中的每个新单元，验证并确认其父辈单 元，父辈单元的父辈单元，慢慢可达创世单元，并将其父辈单元的哈希包含到自己的单元里 面。随着时间递增，所有交易的区块链相互连接，形成图状结构，如若要更改数据，那就不
仅仅是几个区块的问题了，而是整个区块图的数据更改。DAG
这个模式相比来说，要进行 的复杂度更高，更难以被更改。

DAG（有向无环图）是不同于区块链的一种分布式账本技术，是数字资产界的一次较 大的创新。得出以上结论在于：DAG
技术给予高并发的交易提供了解决方案，把区块链二 维的模式提升到三维（即人人皆可为矿工）例如著名的数字货币以太坊ETH就采用了DAG。

什么是 DAC?

在当前以□特币为代表的区块链系统中，SHA-256 哈希计算和 ECDSA 椭圆曲线密码 构成了□特币系统最基础的安全保障，但随着量□计算机技术不断取得突破，特别是以肖□ 算法为典型代表的量□算法的提出，相关运算操作在理论上可以实现从指数级别向多项式级 别的转变，这些对于经典计算机来说□够“困难”的问题必将在可预期的将来被实□型量□ 计算机破解。

后量□密码（post-quantumcryptography），又被称为抗量□计算密码（quantum-resistantcryptography），是被认为能够抵抗量□计算机攻击的密码体制。 量子计算是建造计算机的新方式——利用粒子的量子属性以与传统计算机非常不同的方式在数据上执行操作。在某些情况下，算法加速量非同寻常。正是这种特性使得原来在电 子计算机环境下的一些困难问题，在量子计算机环境下却成为容易计算的。量子计算机的这

种超强计算能力，使得基于计算复杂性的现有公钥密码的安全受到挑战。这就是量子攻击。 抗量子攻击意味着什么呢？ 目前的绝大部分算法，都无法抵挡量子攻击。意味着用户的所有的信息，都将会暴露在量子计算机的面前。如果有了抗量子攻击算法，意味着个人的信息得到最安全的保障，至少以目前的技术手段是无法破解的。抗量子攻击算法意味着安全。

抗量子攻击算法如果研发成功并成功应有于 GMCC，这将会是第一个数字货币行业采 用抗量子攻击算法的数字货币，对数字货币行业和其他数字货币的影响都是深远而具有划时 代的意义的。

而抗量子攻击算法也是 GMCC 的七大技术的其中一个，是 GMCC 区别于其他资产数 字化平台的显著特点之一，同时对 GMCC 的投资者也是一个巨大的提升。

备注：本文首发于百度百家号，内容根据本人对区块链知识的理解以及部分互联网作者总结的很好借鉴来