共识算法（ POW,POS,DPOS,PBFT ）介绍

POW ：Proof of Work ，工作证明。

比特币在 Block 的生成过程中使用了 POW 机制，一个符合要求的 Block Hash 由 N 个前导零构成，零的个数取决于网络的难度值。要得到合理的 Block Hash 需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的 Block Hash 值，说明该节点确实经过了大量的尝试计算，当然，并不能得出计算次数的绝对值，因为寻找合理 hash 是一个概率事件。当节点拥有占全网 n% 的算力时，该节点即有 n/100 的概率找到 Block Hash 。

POS：Proof of Stake ，股权证明。

POS：也称股权证明， 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。

DPOS：Delegated Proof of Stake ，委任权益证明

比特股的 DPoS 机制，中文名叫做股份授权证明机制（又称受托人机制），它的原理是让每一个持有比特股的人进行投票，由此产生 101 位代表 ，我们可以将其理解为 101 个超级节点或者矿池，而这 101 个超级节点彼此的权利是完全相等的。 从某种角度来看， DPOS 有点像是议会制度或人民代表大会制度。 如果代表不能履行他们的职责（当轮到他们时，没能生成区块），他们会被除名，网络会选出新的超级节点来取代他们。 DPOS 的出现最主要还是因为矿机的产生，大量的算力在不了解也不关心比特币的人身上， 类似演唱会的黄牛， 大量囤票而丝毫不关心演唱会的内容。

PBFT：Practical Byzantine Fault Tolerance ，实用拜占庭容错算法。见前文拜占庭容错算法介绍。

PBFT 是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。 每个状态机的副本都保存了服务的状态， 同时

也实现了服务的操作。将所有的副本组成的集合使用大写字母 R 表示，使用 0 到|R|-1 的整数表示每一个副本。为了描述方便，假设 |R|=3f+1 ，这里 f 是有可能失效的副本的最大个数。尽管可以存在多于 3f+1 个副本，但是额外的副本除了降低性能之外不能提高可靠性。

以上主要是目前主流的共识算法。

从时间上来看，这个顺序也是按该共识算法从诞生到热门的顺序来定。

对于 POW，直接让比特币成为了现实，并投入使用。而 POS 的存在主要是从经济学上的考虑和创新。 而最终由于专业矿工和矿机的存在， 让社区对这个标榜去中心化的算法有了实质性的中心化担忧，即传闻 60％～70% 的算力集中在中国。因此后来又出现 DPOS，这种不需要消耗太多额外的算力来进行矿池产出物的分配权益方式。 但要说能起到替代作用， DPOS 来单独替代 POW，POS 或者 POW＋POS 也不太可能，毕竟存在即合理。每种算法都在特定的时间段中有各自的考虑和意义，无论是技术上，还是业务上。

如果跳出技术者的角度， 更多结合政治与经济的思考方式在里面， 或许还会跳出更多的共识算法，如结合类似 PPP 概念的共识方式，不仅能达到对恶意者的惩罚性质，还能达到最高效节约算力的目的也说不定。

至于说算法的选择，这里引用万达季总的这一段话作为结束：

一言以蔽之，共识最好的设计是模块化 ,例如 Notary ， 共识算法的选择与应用场景高度相关，可信环境使用 paxos 或者 raft，带许可的联盟可使用 pbft ，非许可链可以是 pow，pos，ripple 共识等， 根据对手方信任度分级，自由选择共识机制，这样才是真的最优。