区块链的核心问题是共识机制，所有的区块都会采用一种共识机制来保障去中心化网络的同步。可以说，区块链领域内，一切都是围绕共识机制运转的。共识机制的存在的价值，就如同法律对于国家一般。那共识机制到底是什么呢？

共识机制，就是分布式系统的一个过程，一般用在涉及多个不可靠节点的网络中，实现所有节点之间数据一致性并对某一个提案达成一致的协议。不同的共识机制有不同的优缺点。一般判定某一个共识机制的优劣主要以安全性、扩展性、TPS性能、资源消耗这几个方面。

区块链项目虽多，但使用的共识机制无非就哪几种。主流的共识机制一般是POW和POS。

1. POW

所谓的POW，就是工作量证明（proof of work），POW机制主要用于比特币和其他需要挖矿币种的通用机制，对于重复性小概率事件，出示结果就是证明了工作量。即工作量越多，收益越大。

工作量证明这种思想在我们生活中广泛使用。就拿目前火爆的“吃鸡”游戏来说吧，玩家想要生存到最后吃鸡是很小的概率，如果一个人吃鸡次数很多，在排除外挂的前提下，基本上可以认定他的实力很强，吃鸡靠的不是运气；关于运动技巧的掌握，其实也是一种工作量证明。一个田径运动员突破常人的极限，除了本身的天赋之外，一定是付出了大量的时间去练习的，所以工作量和技能的熟练度是成正比的。

2．POS

所谓的POS，就是股权证明机制（proof of stake），与工作量证明机制POW不同之处在于，POS是不必挖矿的，它会在创世区块中写明股权，直接证明你的股份。简单的说，就是你拥有10%的股权，和POW中你拥有10%的算力效果是等同的。

POW与POS两者有哪些优点呢？它们在安全性问题上各有其独到之处。在POW中，获得激励的概率基本等同于占有的算力，因此撒谎的收益明显低于诚实挖矿。在POW中，挖矿者是保障比特币安全的主体，持有者并不会对比特的安全问题有任何影响；POS的安全在于持股股东是不会选择放掉自己手中的钱，于是在这个机制下，不占有POS股权的人不会对链构成威胁，安全取决于股权持有者，与其他的因素毫无关联。

POW和POS都不是完美的。POW是一种赢家通吃的游戏，这会导致大量的算力浪费，而POS从本质上来说就是不公平的，少数人持有大量加密货币，新货的POS的能力受到已经持有POS的绝对限制。

于是又在POS的基础上诞生了新的DPOS机制。DPOS大致原理类似POS，区别在于D,DPOS有点类似于董事会投票。以EOS为例，所有持币地址选出21个超级节点来行使记账权力，如果在规定的时间内没有完成，网络就会选出新的节点取代久的节点。这样的好处是大大减少参与验证和记账的节点数量，比特币出块时间为十分钟，而EOS则能达秒级。

这样的缺点就是没有秉承区块链去中心化理念，顶多只能算是弱中心化。并且大多数的持币者并不关心投票问题，也没有时间、经验和技能。

实用拜占庭容错算法PBFT（Practical Byzantine Fault Tolerance），它主要依据法定多数的决定，每个节点代表着一个票数，以少数服从多数的方式实现了拜占庭的容错演算。优点在于保证灵活性和安全性的前提下最大允许(n-1)/3故障节点的容错性，缺点是当有1/3或以上记账人停止工作后，系统将会停止服务。