分布式共识（distribute consensus）

分布式共识协议 在一个有n个节点的系统中，每一个节点都有一个输入值，其中一些节点具有故障，甚至是恶意的，一个分布式共识协议有以下两个属性：

输入值的终止须经所有诚实节点来确定

这个输入值必须由诚实节点来生成

**所有的节点如何对一个区块达成共识呢？**

一个方法是，在一个时间段里，比如隔十分钟，每个节点都提议，自己的未被认可的交易成为已经达成共识的区块链后后面的下一区块，然后那些节点会执行一些共识协议，每个节点把自己提议的区块作为输入。

但不可避免地，有些节点可能是恶意的，存心要把不正当的交易放入区块里，其他节点则是诚实的。如果共识协议能顺利完成，一个正当有效的区块会被选做输出值。

尽管有些被选出的区块是由一个节点提交的，但只要这个区块是正当有效的，输出就是正当有效的。

这时可能有人指出，这个被选出的区块可能未包含所有的正当有效的交易，但这没有关系，如果有些正当有效的区块没被放进区块，它们可以等待下一次机会。

以上做法有几个技术上的问题：

第一，达成共识一般是一个难题，因为有些节点会死机或是根本就是恶意节点

第二，就比特币而言，点对点网络是不完美的，并非所有对应的节点是两两相连的，互联网链接的不良可能会造成网络问题，要执行一个所有节点都参与的共识协议好像并不现实

第三，由于交易信息是分布在整个互联网上，信息传递会有严重延迟。

不可能性结论

拜占庭将军问题（Byzantine Generals Problem）

Fischer-lynch-Paterson不可能结果，该结果指出，在 一定的条件下（包括节点行为具有确定性特征），甚至在只有一个缺陷的过程中，达成共识都是不可能的。

比特币到底打破了经典模型里的哪些假设呢？

第一，比特币引进了奖励的理念，这对分布式共识协议来说是一个全新的理念，这也只有在比特币里才能实现，因为比特币也是货币，所以人们自然而然地会为了金钱奖励而变得诚实起来。所以，比特币并没有真正解决分布式共识问题，它只是在特定货币系统下解决了这个问题而已。

第二，比特币体系包含随机性这个概念，比特币的共识算法很大程度上依赖于随机性。此外，它也不再纠结于规定共识的起点与终点。相反，共识是通过一段较长的时间而达成的，在实际系统中，达成共识大约需要一个小时左右。但即使在一个小时之后，节点也无法确定哪一个交易块应该进入总帐本。但随着时间的流逝，我们对某一个块的认识与最终总体共识相吻合的概率越来愈大，观点出现分歧的概率按指数级下降。比特币在以上方面的不同，让它能逾越传统理论关于分布式共识不可达成这一鸿沟。

隐性共识（inplicit consensus）

这个算法的简化假设是，可以随意选择一个节点，这些节点都不会受到女巫攻击的影响

1.新的交易被广播到所有节点上

2.每个节点都将新的交易放入一个区块

3.在每个回合，一个随机的节点可以广播它的区块1

4.其他节点可以选择接受这个区块，前提是如果区块里的交易都是正当的（有真的签名）

5.节点们可以把以上区块的哈希值放进自己的区块里，以此来表示它们对那个新区块的认可。