区块链（Blockchain）是比特币的一个重要概念，它本身是一种新型的分布式系统，并且极大的促进了分布式计算领域的发展。了解分布式系统的工作原理，了解共识机制如何使人们在分散的网络上达成共识，我们才能真正了解区块链技术的创新和未来发展的方向。

一、什么是分布式系统？

分布式系统是一种通过网络进行通信使用多台服务器来协同完成计算任务的系统，是一种提高业务承载量的基本手段，通过利用更多的服务器，来解决单个服务器无法同时承载大量的用户使用的问题。

二、分布式系统的优势和面临的挑战

分布式系统的优势

与集中式系统相比，分布式系统有4个方面的优势：

1.性价比更高

随着技术的发展，小型CPU越来越廉价，这使得分布式系统使用多个廉价CPU的方式比使用单个大型CPU性价比更高。

2.总计算能力更强

单个CPU的性能目前还是有一定极限的，但使用分布式系统我们则能够获得比单个CPU更强的总计算能力。

3.固有的分布性

有一些应用本身就是具有分布性的，所以需要分布式系统来满足需求。

4.系统更可靠

单一CPU一旦故障就会100%停机，但分布式系统有一台机器故障其他机器并不受影响，因而分布式系统更为可靠。

尽管分布式系统有诸多优点，但也面临着诸多的挑战：

1. 异构的机器与网络难以协调

分布式系统中的机器，有可能配置不同，其上运行的语言，架构也不相同，因此各节点处理能力不一，同时由于各节点通过网络连接，不同运营商的网络情况也不一样，导致如何协调众多机器共同完成目标成为不小的挑战。

2. 独立进程故障

在现实中，每个进程都有一定的概率发生故障，虽然单一进程的故障概率较低，但分布式系统由于节点数目较多，故障概率就随着节点的增多而变高了。

因此分布式系统需要挑战如何监控每一个节点，保障故障时将该节点的任务转移，从而避免独立进程故障对整个系统的影响。

3. 不可靠的网络

在分布式计算机系统中，时间和事件顺序是一大障碍。

不同节点通过网络连接，但网络并不可靠，我们无法确定网络是否会有延时，乱序等问题，而这些问题很大程度会影响最终的结果。

总的来说，分布式系统的挑战来自于各种不确定因素，流程和节点的增加导致了不确定性概率的增加，如何保证在诸多的不确定下系统还能正常运作是分布式系统必须要解决的问题。

三、分布式系统中的共识问题

为了保障分布式系统的不同节点能够得到统一，我们需要引入共识机制。

所谓“共识机制”，是通过特殊节点的投票，在很短的时间内完成对交易的验证和确认；对一笔交易，如果利益不相干的若干个节点能够达成共识，我们就可以认为全网对此也能够达成共识，也就是说，处于不同情况下的各个节点能够得到统一。

四、常见的共识机制

共识机制是区块链技术的重要组件，区块链技术正是运用一套基于共识的数学算法，在机器之间建立“信任”网络，从而通过技术背书而非中心化信用机构来进行全新的信用创造。

现今区块链的共识机制可分为三大类：工作量证明机制、权益证明机制、股份授权证明机制。

工作量证明机制PoW(Proof of Work)：

工作量证明机制即对于工作量的证明，在基于工作量证明机制构建的区块链网络中，节点通过计算随机哈希散列的数值解争夺记账权，求得正确的数值解以生成区块的能力是节点算力的具体表现。就像“按劳取酬”，你提供了多少算力，就能够获得多少回报。

PoW的优势：

具有完全去中心化的优点，理论上实现了相对公平，每个节点自由进出，都有做出贡献和获得回报的机会，同时破坏系统需要付出极大的成本。

PoW的不足：

基于工作量证明机制的挖矿行为造成了大量的资源浪费，目前达成共识所需要的周期也较长，不适合商业应用。

同时由于市场的趋利性，为了获取更多收益，人们开始建立中心化的矿池矿场，背离了去中心化的初衷，网络安全也逐渐受到威胁。

权益证明机制PoS(Proof of Stake):

与要求证明人执行一定量的计算工作不同，权益证明要求证明人提供一定数量Token的所有权即可。权益证明机制的运作方式是，当创造一个新区块时，矿工需要创建一个“币权”交易，交易会按照预先设定的比例把一些Token发送给矿工本身。

也就是，你的挖矿收益，取决于你Token的多少与持有的时间，你持有的越多你的收益就越大。

PoS的优势：

相对于PoW更加节能，不需要耗费大量能源去挖矿。

PoS根据每个节点拥有Token的比例和时间，依据算法等比例地降低节点的挖矿难度，从而加快了寻找随机数的速度，能在一定程度上缩减达成共识的时间。

同时和PoW一样，破坏系统的成本较高。

PoS的不足：

PoS模式下，Token只能通过融资方式发行，无法保障持有者不因受利益诱惑而抛售，同时这种模式的信用基础不够牢固，也并没有从根本上解决难以应用于商业领域的问题。

股份授权证明机制DPoS（Delegated Proof of Stake）：

股份授权证明机制是一种新的保障网络安全的共识机制。与董事会投票类似，该机制拥有一个内置的实时股权人投票系统，全体节点投票选举出一定数量的节点代表，由他们来代理全体节点确认区块、维持系统有序运行。同时，区块链中的全体节点具有随时罢免和任命代表的权力。

DpoS的优势：

大大缩减了参与验证记账的节点数量，能耗更低，同时极大的缩短了共识验证需要的时间。

同时由全体节点投票选择节点代表的机制理论上比PoW,PoS更加去中心化，不容易被操纵。

DPoS的不足：

DpoS理论上更加去中心化，但由于大部分节点因为种种原因投票积极性不高或不便投票，共识掌握在少数的节点代表手中，对于一些节点代表作恶的行为也不能够及时的响应，有较大的安全隐患。

结合以上内容我们可以发现，目前的共识机制都不是完美的，在应用场景上都有一定的限制。

融数链认为：区块链共识机制，仍在不断地发展进化当中，现在的我们需要结合实际的应用场景来选择适合的共识算法，并且根据实际的需要进行改进，逐步解决区块链难以运用于商业领域的问题。