拥有多年的区块链服务经验，为用户提供专业的服务信息，下面介绍POW、POS、POC等共识机制及代表币种详细解读，以及pow机制的币，选择可以为您随时随地解决玩币中所遇到的各种问题，让你不再为职称评级繁琐事务而烦恼。

区块链是建立在P2P网络，由节点参与的分布式账本系统，最大的特点是“去中心化”。也就是说在区块链系统中，用户与用户之间、用户与机构之间、机构与机构之间，无需建立彼此之间的信任，只需依靠区块链协议系统就能实现交易。

可是，要如何保证账本的准确性，权威性，以及可靠性？区块链网络上的节点为什么要参与记账？节点如果造假怎么办？如何防止账本被篡改？如何保证节点间的数据一致性？……这些都是区块链在建立“去中心化”交易时需要解决的问题，由此产生了共识机制。

所谓“共识机制”，就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；当出现意见不一致时，在没有中心控制的情况下，若干个节点参与决策达成共识，即在互相没有信任基础的个体之间如何建立信任关系。

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。

不同的区块链种类需要不同的共识算法来确保区块链上最后的区块能够在任何时候都反应出全网的状态。

目前为止，区块链共识机制主要有以下几种：POW工作量证明、POS股权证明、DPOS授权股权证明、Paxos、PBFT（实用拜占庭容错算法）、dBFT、DAG（有向无环图）

下面我们主要说说常见的POW、POS、DPOS共识机制的原理及应用场景

概念：

工作量证明机制（Proof of work ），最早是一个经济学名词，指系统为达到某一目标而设置的度量方法。简单理解就是一份证明，用来确认你做过一定量的工作，通过对工作的结果进行认证来证明完成了相应的工作量。

工作量证明机制具有完全去中心化的优点，在以工作量证明机制为共识的区块链中，节点可以自由进出，并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。

应用：

POW最著名的应用当属比特币。在比特币网络中，在Block的生成过程中，矿工需要解决复杂的密码数学难题，寻找到一个符合要求的Block Hash由N个前导零构成，零的个数取决于网络的难度值。这期间需要经过大量尝试计算（工作量），计算时间取决于机器的哈希运算速度。

而寻找合理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。在节点成功找到满足的Hash值之后，会马上对全网进行广播打包区块，网络的节点收到广播打包区块，会立刻对其进行验证。

如果验证通过，则表明已经有节点成功解迷，自己就不再竞争当前区块，而是选择接受这个区块，记录到自己的账本中，然后进行下一个区块的竞争猜谜。网络中只有最快解谜的区块，才会添加的账本中，其他的节点进行复制，以此保证了整个账本的唯一性。

假如节点有任何的作弊行为，都会导致网络的节点验证不通过，直接丢弃其打包的区块，这个区块就无法记录到总账本中，作弊的节点耗费的成本就白费了，因此在巨大的挖矿成本下，也使得矿工自觉自愿的遵守比特币系统的共识协议，也就确保了整个系统的安全。

优缺点

优点：结果能被快速验证，系统承担的节点量大，作恶成本高进而保证矿工的自觉遵守性。

缺点：需要消耗大量的算法，达成共识的周期较长

概念：

权益证明机制（Proof of Stake），要求证明人提供一定数量加密货币的所有权。

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币发送给矿工本身。权益证明机制根据每个节点拥有代币的比例和时间，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。

应用：

2012年，化名Sunny King的网友推出了Peercoin（点点币），是权益证明机制在加密电子货币中的首次应用。PPC最大创新是其采矿方式混合了POW及POS两种方式，采用工作量证明机制发行新币，采用权益证明机制维护网络安全。

为了实现POS，Sunny King借鉴于中本聪的Coinbase，专门设计了一种特殊类型交易，叫Coinstake。

上图为Coinstake工作原理，其中币龄指的是货币的持有时间段，假如你拥有10个币，并且持有10天，那你就收集到了100天的币龄。如果你使用了这10个币，币龄被消耗（销毁）了。

优缺点：

优点：缩短达成共识所需的时间，比工作量证明更加节约能源。

缺点：本质上仍然需要网络中的节点进行挖矿运算，转账真实性较难保证

概念：

授权股权证明机制（Delegated Proof of Stake），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，就像系统随时都在召开一个永不散场的股东大会，所有股东都在这里投票决定公司决策。

授权股权证明在尝试解决传统的PoW机制和PoS机制问题的同时，还能通过实施科技式的民主抵消中心化所带来的负面效应。基于DPoS机制建立的区块链的去中心化依赖于一定数量的代表，而非全体用户。在这样的区块链中，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。如果必要，全体节点可以通过投票让现任节点代表失去代表资格，重新选举新的代表，实现实时的民主。

应用：

比特股（Bitshare）是一类采用DPOS机制的密码货币。通过引入了见证人这个概念，见证人可以生成区块，每一个持有比特股的人都可以投票选举见证人。得到总同意票数中的前N个（N通常定义为101）候选者可以当选为见证人，当选见证人的个数（N）需满足：至少一半的参与投票者相信N已经充分地去中心化。

见证人的候选名单每个维护周期（1天）更新一次。见证人然后随机排列，每个见证人按序有2秒的权限时间生成区块，若见证人在给定的时间片不能生成区块，区块生成权限交给下一个时间片对应的见证人。DPoS的这种设计使得区块的生成更为快速，也更加节能。

DPOS充分利用了持股人的投票，以公平民主的方式达成共识，他们投票选出的N个见证人，可以视为N个矿池，而这N个矿池彼此的权利是完全相等的。持股人可以随时通过投票更换这些见证人（矿池），只要他们提供的算力不稳定，计算机宕机，或者试图利用手中的权力作恶。

优缺点：

优点：缩小参与验证和记账节点的数量，从而达到秒级的共识验证

缺点：中心程度较弱，安全性相比POW较弱，同时节点代理是人为选出的，公平性相比POS较低，同时整个共识机制还是依赖于代币的增发来维持代理节点的稳定性。

目前主要有四大类共识机制：Pow、Pos、DPos、Pool

1、Pow工作量证明，就是大家熟悉的挖矿，通过与或运算，计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储；

优点：完全去中心化，节点自由进出；

缺点：目前bitcoin已经吸引全球大部分的算力，其它再用Pow共识机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长，不适合商业应用

2、Pos权益证明，Pow的一种升级共识机制；根据每个节点所占代币的比例和时间；等比例的降低挖矿难度，从而加快找随机数的速度。

优点：在一定程度上缩短了共识达成的时间

缺点：还是需要挖矿，本质上没有解决商业应用的痛点

3、DPos股份授权证明机制，类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。

优点：大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证

缺点：整个共识机制还是依赖于代币，很多商业应用是不需要代币存在的

4、Pool验证池，基于传统的分布式一致性技术，加上数据验证机制；是目前行业链大范围在使用的共识机制

优点：不需要代币也可以工作，在成熟的分布式一致性算法（Pasox、Raft）基础上，实现秒级共识验证；

缺点：去中心化程度不如bictoin；更适合多方参与的多中心商业模式

在使用共识机制，保证数据一致性时的巨大优势（共识机制则是Ripple首先提出的，数据正确性优先的网络交易同步机制，在共识网络中，无论软件代码怎么变动，无法取得共识就无法进入网络，更不要提分叉了）。

———————————————————————

PS：稍微自黑下，虽然共识机制绝对能确保任何时候都不会产生硬分叉。但是，这种机制的缺点也比较明显，那就是要取得与其他节点的共识，明显要比当前Bitcoin网络漫长的多。极端情况下，在Ripple共识机制网络中掉线的后果也是很恐怖的。

有可能你家停电一天，第二天整个系统就再也无法与其它Rippled节点取得共识了（共识机制事实上需要超过80%的节点承认了你的数据，你的提交才会被其它节点接受，否则就会被排它的拒绝连接），甚至只能清空自己全部500多GB数据重新同步才能连上其它Ripple节点。

所以目前来说，现有的Rippled端并不适合民用（商用的话影响就比较小，比如RL自己的Rippled节点托管在亚马逊云数据中心，长时间无响应是可以高额索赔的，而且那种地方除了大型灾害几乎不会断），这也是RL一直想改进的方面之一。

POW：Proof of Work，工作证明。比特币在Block的生成过程中使用了此机制，找到合理的Block Hash需要经过大要得量尝试计算，计算时间取决于机器的哈希运算速度。POS：Proof of Stake，股权证明。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POS模式下，持币有利息。DSC（动态权益）共识算法：公链项目Penta的独创。分三层：第一层进行代表选举，第二层通过三列筹钱算法挑选议员和观察员组成若干共识组，第三层从候选区块中通过散列抽签算法选取正式

块。

这个不好说，理论上应该pow更有利于价格的问题。不过，也要具体问题具体分析，以太坊都计划采用POS机制。

在很多社区的讨论中，在许多人的眼里，似乎把POS（Proof of Stake，权益证明）和POW（Proof of work，工作量证明）视为完全对立的两种证明方式，POW是中本聪最早提出的工作量证明方式，而POS是目前许多二代币逐渐采用的方式。

而DPOS则是DPOS机制似乎又重新把权利归还到那些持有数字货币的人手上。但是目前比较成功的币种都是采用POW，例如比特币、DECENT、狗狗币等等。

都是区块链的底层共识算法，POW费电。EOS用的DPOS，21个超级节点，但是老贿选，所以现在DPOS基本上被扣上了中心化区块链的帽子，我也觉得这样违背区块链精神。POR共识协议是最新由贝克链提出的一种共识机制，由公钥之父、图灵奖得主Whitfield Diffie的Cryptic Labs孵化，这个实验室是世界上最牛的网络安全实验室。

什么是共识机制？

我在开更的第一篇文章，就简单讲解了数字货币世界的16个最高频名词，其中一个就是共识机制，还记得吗？

为什么要有共识机制呢？

这就必须要解释一下在分布式系统中不得不了解的“拜占庭将军问题”了。

拜占庭将军问题（The Byzantine Generals Problem）可以总结为一句话：

在古代，11位忠诚的、不同位置的将军，如何排除叛徒的影响，对进攻或撤退达成一致。

当然，拜占庭将军问题并不是如今才提出的，我们大中华在春秋战国时期就发明了“虎符”这个神奇的方式来保障命令的正确执行。

在分布系数系统中，各个节点就是“拜占庭将军”，算法执行中的任意一个错误就是“叛徒”。

为了尽可能地排除错误、快速达成一致，来让系统有效地、正确地运行，便应运而生了各种“共识机制”。

———————————————————

下面，我们就来一起学习数字货币世界中常见的几种共识机制：

PoW，工作量证明 Proof of Work

PoW是比特币所采用的共识机制，最早是由Adam Back为了解决垃圾邮件的问题而开发的一个“哈希现金Hashcash”程序。

比特币采用的是SHA256的单向函数，其具体的工作原理实在太专业，我们只需要理解到“SHA256的结果很容易验证，但是要将其计算出来，需要不断尝试运算，直到匹配到某个随机数；技术上而言，任何新增区块都需要经过232394亿运算才能得到”的程度，感兴趣的小伙伴可以搜索SHA256去深入学习。

因此，只要矿工出示运算结果，那通过PoW，全网节点就认可了他所付出的成本，承认新的区块奖励属于他。

如此大量的运算相当浪费资源，实际上并没有任何科学或实际用途，只是为了实践工作量证明机制、阻止攻击者伪装成节点来控制网络。

虽然在2009年时为了构建这种去中心化的、允许所有人可以免费参与的全球货币网络，没有更好的选择；但是发展到如今，已经有了其他不需要大量浪费算力的证明机制，比如我们下面就要提到的，PoS权益证明。

———————————————————

PoS，权益证明 Proof of Stake

主要思想是：节点记账权的获得难度与节点持有的权益成反比，也就是说，一个节点拥有的币越多、时间越久，越容易获取记账权，也就越容易获取区块奖励。

实际上，最初的PoS是PoW的一种升级，根据每个节点的币龄，来等比例地降低挖矿难度，从而加快找到随机数的速度。

什么是币龄呢？

币龄=数量*拥有天数。

由于区块链中的每笔交易记录都会被标记时间戳，这个时间戳就可以作为币龄的证明，因此币龄也不可能被轻易伪造。

比如A从B那里收到10个币，并且持有了90天，那么，A就拥有了900的币龄；如果A卖了这10个币，这900币龄就被消耗了；

后来，为了彻底摆脱PoW这种依靠算力的共识机制，PoS引入了“利息”的概念；年利率是在PoS机制最初确认时就设定的，一般不会变化。

利息=（币龄*年利率）/365
，如果利率是1%，在上个例子中，A就可以得到0.02466个币的利息。

如此一来，PoS区块链的作用过程就可以这样描述：

在初期，通过PoW机制，产生创世币；

在创世币达到一定规模时，PoS机制开始作用，交易时消耗币龄、获得产生区块的优先权，并获取利息，同时PoW机制由于消耗太多资源、浪费算力而逐渐淡出；

最终系统中仅剩PoS来维持正常运作。

目前大家所熟悉的以太坊，主要还是采用PoW的机制，不过正在转向PoS。

————————————————————

大家了解了PoW和PoS，在遇到其他共识机制的时候，相信也会比较快得就能理解。

比如：股份授权证明DPOS，类似于董事会投票；燃烧证明POB；沉淀证明POD；能力证明POC；消逝时间证明PODT，等等。

就不在这里为大家一一展开了，感兴趣的同学可以百度或知乎一下~

感谢您阅读本篇对POW、POS、POC等共识机制及代表币种详细解读的详细介绍，如果你对pow机制的币还不够了解，想进一步学习关于POW、POS、POC等共识机制及代表币种详细解读的知识，可以在本站首页搜索你想知道的！