

众所周知，区块链的主要技术就是节点竞争进行记账，而竞争就要有裁判，而共识机制就相当于竞争众多裁判，现如今不同的区块链采用的可能就是不同的共识机制，因此市面上的共识机制有很多，其中最为常见的就是pow共识机制和pos共识机制，而本文主要跟大家了解的是pos共识机制，那么，POS共识机制到底是什么意思呢？下面小编就给大家详细的POS共识机制是什么意思？希望通过本文的介绍，投资者能对pos共识机制有所了解。

POS共识机制是什么意思？

权益证明机制(Proof of Stake)，简称POS，也称股权证明机制，类似于把资产存在银行里，银行会通过你持有数字资产的数量和时间给你分配相应的收益。

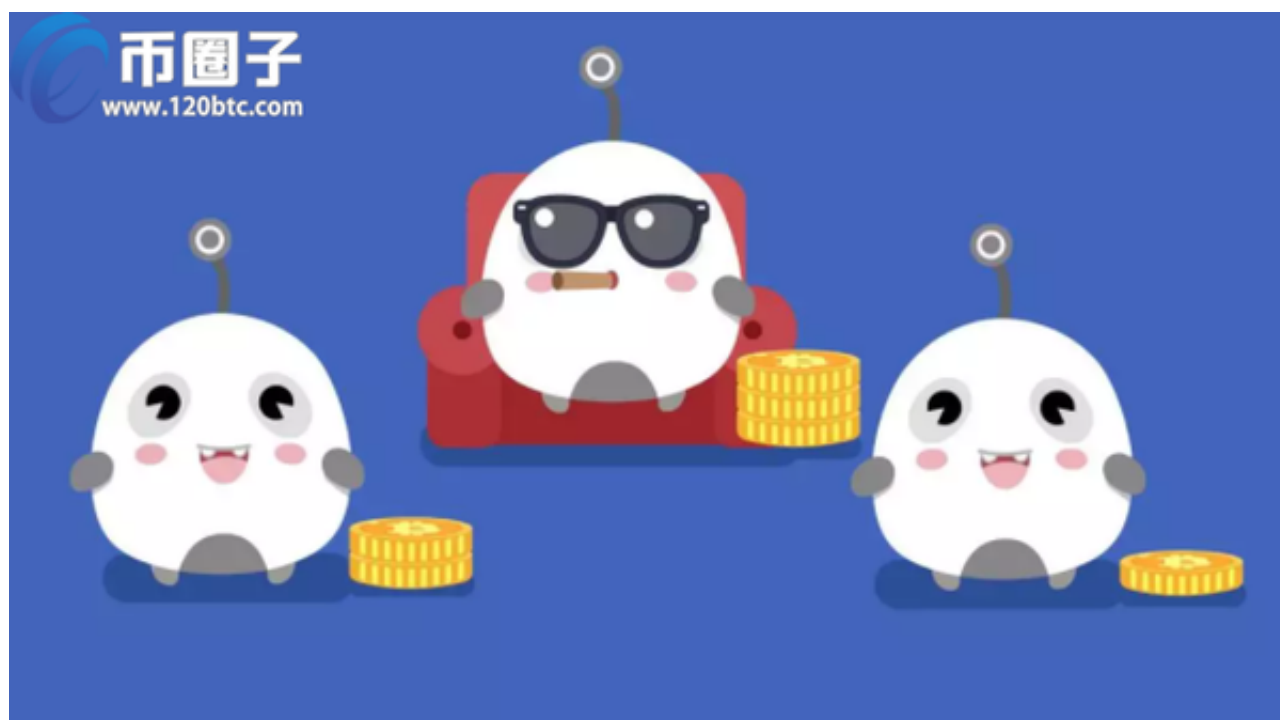
同理，采用PoS的数字资产，系统根据你的币龄给你分配相应的权益，币龄是你持币数量 and 时间的乘积。比如你持有100个币，总共持有了30天，那么，此时你的币龄就为3000。

相较PoW(工作量证明机制)，PoS存在2个优势。第一，PoS不会造成过多的电力浪费，因为PoS不需要靠比拼算力挖矿。第二，POS更难进行51%攻击。拥有51%币才能发起攻击，网络受到攻击却会造成自己利益受损，显然很不划算。

目前，有很多数字资产用PoW发行新币，用PoS维护区块链网络安全。

POS共识机制工作原理：

PoS机制主要是通过权益记账的方式，来解决网络的效率低下、资源浪费和各节点的一致性问题，简单来说，就是谁拥有的权益多谁说了算。它的原理是这样的：



PoW之所以有种种问题，主要是因为人人都可以自由地成为节点，而每个节点又通过竞争的方式参与数据处理。一笔数据要经过这么多人的处理，肯定会造成资源浪费和效率低下。

PoS之所以能解决这个问题，是因为PoS提高了节点处理数据的门槛，它规定：虽然每个人都可以自由地加入进来成为节点，但只有满足一定条件的节点，比如抵押一定数量的代币，才有资格成为验证节点，也就是候选人。



成为候选人后，系统会通过算法，选择一部分人作为出块节点，每隔一段时间，会重新选择，选取过程中，算法会保证选取的结果不能被操纵，也不能被预测，从而避免网络被某一节点所控制。只有成为出块节点，也就是矿工，才能参与数据的处理、争夺记账的权利。

所以说PoW是人人都可以成为矿工，而PoS则是通过一系列筛选，才能成为矿工。

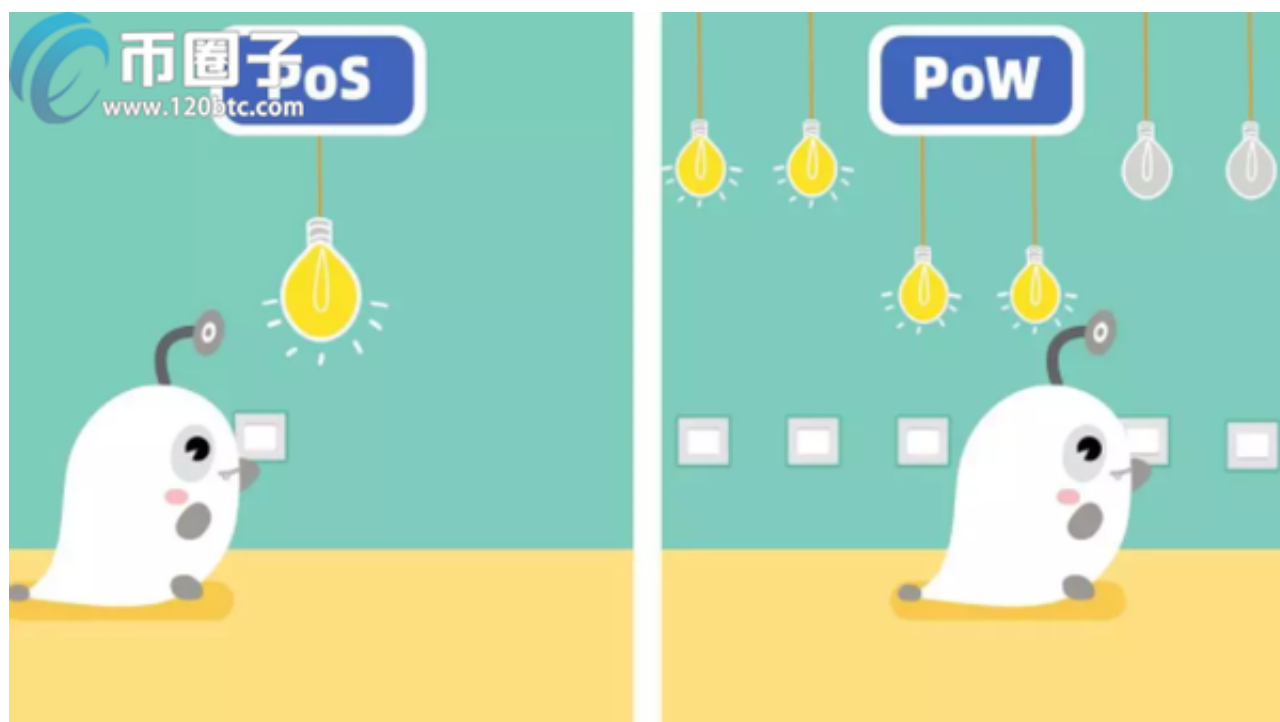


PoS具体的竞争方式是，谁持有的代币多，谁就越容易获得出块的权利。然后通过全网广播，他打包的区块经其他矿工验证，确认没问题后，这个区块就会连接到链上，并同步在全网其他节点的小账本中，同时他获得相应的代币奖励。



整个流程简单总结起来就是：持币人将代币抵押，获得出块的机会，然后PoS共识中会通过选举算法，按照持币量比例，从中选出出块矿工。矿工在指定高度完成打包交易，生成新区块，并广播区块，广播的区块经过验证人验证交易，通过验证后，区块得到确认。这样一轮PoS的共识过程就完成了。

PoS机制的优势在于，它解决了PoW中的资源浪费、效率低下等问题。但它同样也有一些缺点。比如，PoS机制中初始的代币分发比较模糊，如果初始代币分发不下去，就很难形成之后的股权证明。再比如，选举算法存在被攻击的可能，一旦攻击成功，整个系统就会被操控。



但是PoS机制最大的问题，还是容易造成强者恒强的局面，谁的代币越多，谁就越容易获得更多的代币，理论上谁能掌握51%的代币，谁就能掌控整个网络，所以，它的去中心化程度要弱一些。

以上就是POS共识机制是什么意思的相关内容介绍，众所周知，从目前的情况来看，PoS协议由于更偏向于用户侧，用户没有大量的硬件投入需求，在逐利的时候，会更偏向于短期的利，而短期的利，很可能对于区块链的基础平台造成损害，甚至有可能使51%攻击发生的更加容易，也就是说从Token经济学角度看PoS共识机制在代码实现的时候，还需要更加仔细的设计。