## ****认识PoW：****

PoW即工作量证明，就是大家熟悉的挖矿，通过数学运算，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。

例如比特币采用的共识算法就是 PoW，专业一点说，矿工们在挖一个新的区块时，必须对SHA-256密码散列函数进行运算，区块中的随机散列值以一个或多个0开始。随着0数目的上升，找到这个解所需要的工作量将呈指数增长，矿工通过反复尝试找到这个解。最先算出正确答案的节点可获得当前区块的记账权，同时获得新发行比特币的奖励。

## PoW的优点

1.去中心化，将记账权公平的分派到其他节点。你能够获得的币的数量，取决于你挖矿贡献的有效工作，也就是说，你用于挖矿的矿机的性能越好，分给你的收益就会越多，这就是根据你的工作证明来执行币的分配方式。

2.安全性高，破坏系统需要投入极大的成本，如果想作弊，要有压倒大多数人的算力(51%攻击)。因为作弊要付出一定成本，作弊者就会谨慎对待了。在比特币的 PoW 机制中，由于获得计算结果的概率趋近于所占算力比例，因此在不掌握51%以上算力的前提下，矿工欺诈的成本要显著高于诚实挖矿，甚至不可能完成欺诈(由于概率过低)。

## PoW的缺点

1.挖矿造成大量的资源浪费，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。这让依据算力公平分配奖励的机制，演变为了对矿机算力的大举投入，扭曲了中本聪的设计初衷，即去中心化。

2.网络性能太低，需要等待多个确认，区块的确认共识达成的周期较长(10分钟)，现在每秒交易量上限是7笔(visa的平均每秒交易量上万，支付宝峰值接近9万)，不适合商业应用。

## 认识PoW

PoS 全称是 Proof of Stake，中文翻译为权益证明。PoS 最早出现在点点币的创始人 Sunny King 的白皮书中，它的目的就是为了解决使用 PoW 挖矿出现大量资源浪费的问题。

在讲 PoS 之前，我先来讲一个叫做币龄的概念，币龄这个概念其实很好理解，它的英文是 CoinAge，字面意思就是币数量乘以天数。比如你有 100 个币，在某个地址上 9 天没有动，那么产生的币龄就是 900，如果你把这个地址上这 100 币转移到任意地址，包括你自己的地址，那么 900 个币龄就在转移过程中被花费了，你的币数量虽然还是 100 个，但是币龄变更为 0。币龄在数据链上就可以取到，任何人都可以验证。

区块链共识机制的第一步就是随机筛选一个记账者，PoW 是通过计算能力来获得记账权，计算能力越强，获得记账权的概率越大。PoS 则将此处的计算能力更换为财产证明，就是节点所拥有的币龄越多，获得的记账的概率就越大。这有点像公司的股权结构，股权占比大的合伙人话语权越重。

## PoS的优点

1.节约能源，不需要大量消耗电力和能源。

2.相比于PoW，PoS机制的加密货币对计算机硬件基本上没有过高要求，不用担心算力集中导致中心化的出现。

3.矿工不需要去拼算力，而且也不会浪费太多的算力，这样间接性的就会缩短达成共识的时间。性能上会比POW要来的高。

4.降低51%攻击的概率

## PoS的缺点

去中心化特性变弱，参与者权益越多，获得记账权机率更大，容易产生垄断。

## 总结

总的来说，每种共识算法都有自己的优势，所以要结合实际应用场景选择适合的算法。

工作量证明PoW主要是依靠计算机性能决定记账，性能越高，就越有机会获取记账的权利；但是这会导致大量资源的浪费。这时权益证明PoS出现了，主要解决 PoW 机制中大量资源被浪费的情况，即参与者持有币的时间越长，难题越简单，挖到币的概率越大；但是容易产生垄断。