今天我们用通俗的例子来对比下POW与POS机制。

POW：有一道数学题非常难算

POW（Proof of Work），工作量证明，引入了对一个特定值的计算工作。

比特币采用的共识算法就是POW，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。

在这其中，如果想要对业已出现的区块信息进行修改，攻击者必须完成该区块外加之后所有区块的工作量，并最终赶上和超越诚实节点的工作量。

用一个通俗的例子来说：

你上学的时候，班级里发生的行为需要被记在班级的一个大家公用的账本（区块链）上。

老师或者同学们用这个公用的账本进行记录，并且有一种专门用来支付这个账本上大家记录的、需要支付的代币，我们暂且把它叫做PLST币。这些币可以兑换成钱。你们班级的公共账本不是一个大本子，而是由很多个小本子中间连接一条线组合成的。

每个小本子的启用需要进行一个数学运算，如果一个同学算出了某个小本子附带的数学题，就开启了一个新的小本子连着前面小本子，大家就会开始用新本子记账。

每个小本子开头都留一页，写上与其他小本子关联的信息、小本子的启用时间和开启这个小本子时算的数学题的答案。

因为同学们学习都很忙，如果没有报酬的话，就没有人会花费大量时间去班级的小本子上帮大家记账，因此老师做了一个规定：最先算出新的小本子附带的数学难题、开启小本子的人获得Good币，用币来奖励维持班级账本正常运转的同学。

一个期末，你得了奖，A同学算出了一个新小本子——第N个小本子带着的数学难题的解，然后帮你得奖的信息记在了小本子上，A同学获得了一笔奖励。

B同学一直不喜欢你，他想把记录在小本子上的信息修改成B同学得奖，这样老师就会把奖金发给他。

B同学开始计算第N个小本子上的数学难题，当他重新计算完第N个上面的数学题，其他同学已经计算出和第N个小本子连着线的第N+1个小本子的解了。

（因为b同学算的慢，其他同学只认最长链，所以b同学算的无效）

其他记账的同学根据最长链原则都跟在了第N+1个小本子的后面，所以B同学除非计算的速度变得很快，跟上另一条并超过，否则没办法将自己修改的错误信息的区块纳入整个账本系统中。

所以POW共识机制的优点之一：B在攻击公共账本的时要耗费大量的时间精力和脑力，但结果却很难成功，所以如果他选择攻击，不仅得不到奖励，还会对自己造成大量的消耗，就会得不偿失——即降低不诚实节点的攻击意图。

但，不得不说的是，攻击存在成功的可能性，如果B同学说服班上超过50%的同学一起承认错误他修改的错误的账本，那么被篡改的账本就会被达成共识。当然，就攻击这个公共账本而言，除非，超过50%的同学用被B同学的一己私欲说服。

以这个例子来看，缺点也很明显，为了维护这个公共账本的运作，班级的同学花费了大量的时间来算这些哈希函数的难题，浪费了大量的时间和精力，表现在比特币上就是：花费了大量的电力，浪费了大量的能源。