**一、什么是POS**

POS是一种在公链中的共识算法，可作为POW算法的一种替换。POW是保证比特币、当前以太坊和许多其它区块链安全的一种机制，但是POW算法在挖矿过程中因破坏环境和浪费电力而受到指责。POS试图通过以一种不同的机制取代挖矿的概念，从而解决这些问题。

POS机制可以被描述成一种虚拟挖矿。鉴于POW主要依赖于计算机硬件的稀缺性来防止女巫攻击，POS则主要依赖于区块链自身里的代币。在POW中，一个用户可能拿1000美元来买计算机，加入网络来挖矿产生新区块，从而得到奖励。而在POS中，用户可以拿1000美元购买等价值的代币，把这些代币当作押金放入POS机制中，这样用户就有机会产生新块而得到奖励。在POW中，如果用户花费2000美元购买硬件设备，当然会获得两倍算力来挖矿，从而获得两倍奖励。同样，在POS机制中投入两倍的代币作为押金，就有两倍大的机会获得产生新区块的权利。

总体上说，POS算法如下所示。存在一个持币人的集合，他们把手中的代币放入POS机制中，这样他们就变成验证者。假设在区块链最前面一个区块（区块链中最新的块），这时POS算法在这些验证者中随机选取一个（选择验证者的权重依据他们投入的代币多少，比如一个投入押金为10000代币的验证者被选择的概率是一个投入1000代币验证者的10倍），给他们权利产生下一个区块。如果在一定时间内，这个验证者没有产生一个区块，则选出第二个验证者来代替来产生新区块。与POW一样，以最长的链为准。

注意这个模型有许多变种。在之前点点币的POS算法中，每秒钟有一个不同的验证者被分配来产生区块。有时，没有一个明确的机制来说明谁成为验证者。每个代币持有人都是一个潜在的验证者，但如果一个代币持有人离线或者对验证不感兴趣，他就会错过产生新区块的机会。而在有些POS算法中，根本没有验证者选择的概念。因此，一种传统的拜占庭容错共识算法过去常常用来使所有验证者同意下一个区块。然而，选择下一个验证者的伪随机算法可以有很多不同方式，但无论充值或其它方式，使用代币替换矿工的原则是不会改变的。

有什么好处？

简而言之：  
不再需要为了安全产生区块而大量消耗电能。  
由于不再需要大量能耗，通过发行新币以激励参与者继续参与网络的压力会下降。理论上负总发行量甚至成为可能，由于一部分交易费“被烧”掉因此货币供应随着时间减少。  
有可能通过“合作博弈论”减少自私挖矿攻击遭成的系统弱点，虽然POW在一定程度上也可以做到这一点。  
随着规模经济（指扩大生产规模引起经济效益增加的现象）的消失，中心化所带来的风险减小了。价值一千万美元的代笔带来的回报不多不少是价值一百万美元代币的10倍，不会有人因为负担得起大规模生产工具得到不成比例的额外回报。  
相较工作证明制度，POS制度中实施经济惩罚的可能会使各种51攻击变得极其昂贵－引用Vlad Zamfir的话说“参加51攻击就好比你的ASIC农场着火了”。

POS（股权证明）如何（加入）传统拜占庭容错研究？

拜占庭容错研究中得出的几个基本结论对所有共识算法普遍适用，包括像PBFT这样的传统共识算法以及任何股权证明（POS，即proof of stake）算法，甚至同流行的看法相反，在一定程度上适用于工作证明算法。

关键结论包括：  
CAP定理－“在网络分区产生的情况下，你必须选择一致性（consistency）或者可用性（availability），无法两项全都满足。“ 直觉上的论证很简单：如果网络分成了两半，并且我在一半的网络中“给A发送了10个币”在另外一半的网络中“给B发送了10个币”，那么要么系统不可用，因为一比交易或者两比都不会被处理，要么系统会变得没有一致性，因为一般的网络会完成第一笔交易，而另外一半网络会完成第二笔交易。

FLP不可能性－在一个异步条件下（也就是说，甚至正常运作的节点之间的网络延时也不存在一个保证的界），即便只有一个错误／不诚实的节点存在那么创造出一种能够保证在有限时间内达成共识的算法就是不可能的。注意这里不排除“拉斯维加斯”算法每轮会具有一定概率达成共识，因此随着时间T的增长在T时间内达成共识的概率会以指数式的速度趋近于1。

容错界限－从DLS论文中我们得出结论：（1）在一个部分同步网络的模型（也就是说：网络延时有界限但是我们并不知道在哪里）下运行的协议可以容忍1/3任意（换句话说，拜占庭）错误，（2）在一个异步模型中的确定性的协议（没有网络延时上限）不能容错（不过这个论文没有提起随机化算法可以容忍1/3的错误），（3）同步模型中的协议（网络延时可以保证小于已知d时间）可以，令人吃惊的，达到100%容错，虽然对1/2的节点出错可以发生的情况有所限制。注意“验证拜占庭”模型是那个值得考虑的模型，而不是“拜占庭”模型；验证的部分基本上意味着我们可以在算法里使用公钥，此行为现在被研究得非常透彻并且已经非常便宜了。

工作证明已经经过Andrew Miller和其他人的严谨分析，它已经被证实在同步网络模型中是一个可靠的算法。例如比特币，假设网络延迟为零，具有50%的容错率，在实际观测中可达～49.5%，但是如果网络延时等于出块时间容错率则降至33%，当网络延时的趋近于无限容错则趋近于零。我们一般意识不到这一点因为比特币的出块时间很长（10分钟），连以太坊14秒出块时间都只有大概46%的容错率，但是从根本上违反拜占庭容错理论的情况尚未出现。值得注意的是，在工作证明的概念里没有N个节点存在的概念，虽然网络可以容忍到0.495\*N个错误。然而，不同节点的运算时间可能不同，算力已经通过抽象化的方式被映射到拜占庭容错的理论框架之中了。

股权证明（POS）共识更明显是一个拜占庭容错共识问题。就像工作证明一样，大多数算法通过依靠同步网络模型来达到50%的容错率。已经存在一些研究，特别是在Tendermint项目里，着眼于创作一种依靠部分同步或者异步网络模型的共识算法。所有工作证明和一些股权证明会选择可用性而不是一致性，虽然Casper的（finality）机制以及Tendermint选择会一致性。

注意Ittay Eyal和Emin Gun Sirer有关自私挖矿的发现，它根据网络模型的不同给比特币挖矿分别设置的25%和33%的动机兼容率上限是跟传统共识算法研究的结果完全无关的，传统研究并不涉及动机兼容的问题。（也就是说，只有共谋不可能大于25%或者33%时挖矿的动机才是兼容的。）