1. PoS共识算法提出背景

工作量证明PoW是08年在中本聪所创造的比特币中提出的，至今已经经过了充分的考验和测试，但随着越来越多的矿工和矿池的加入，挖掘新的区块的难度指数爆发式上升，也面临的如下的问题：

1. 能源消耗比较大，浪费电力
2. 加入挖矿行列需要花大量资金购买设备进入

**显而易见，“挖矿”过程消耗了大量的电力资源，这些能耗是必须的吗？**

矿工挖矿是为了取得出块奖励，获取收益。而系统给予出块奖励的目的是激励矿工参与区块链系统维护，进行记账，而挖矿本质上是看矿工投入资金来决定的(投入资金买设备->设备决定算力->算力比例决定收益)。

那么，为什么不直接拼“钱”呢？现状是用钱购买矿机维护系统稳定，为什么不大家都将钱投入到系统开发和维护中，而根据投入钱的多少来进行收益分配呢？这就是权益证明PoS的基本思想。

实际上，在以太坊的PoW算法被置入了一个叫做“难度炸弹”的机制，目的就是逐渐让以太坊的PoW挖矿变得越来越难，迫使网络转向PoS。

1. PoS

一般来说，采用权益证明的货币，会先预留一些货币给开发者，而开发者也会出售一些货币换取开发所需要的资金，在系统进入稳定状态后，每个人都安装持有货币的数量进行投票。优点：

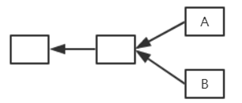
1．省去了挖矿的过程，也避免了因此产生的能耗和对环境影响，减少了温室气体的排放。

2. 维护区块链安全的资源形成闭环，而POW中维护其安全的资源需要通过现实中流通的货币购买矿机等设备进去区块链的，这也就导致只要有人想要攻击，只需要外部聚集足够资金就可以攻击成功(小型币种很容易被攻击，也就是在摇篮里就扼杀掉)。可见，POS机制可以有效防御这种情况(攻击PoS系统需要大量买入该种数字货币，攻击该系统相当于攻击自己)。

|  |
| --- |
| 有些币种根据持有币的权益进行挖矿难度调整(实际并不能这么简单设置，因为会导致资本越多做容易挖矿，因此需要添加一定限制)，也就是结合POW和POS。可见，POS与POW并不互斥。 |

当然，权益证明这么好，为什么实际中并未得到大规模应用呢？原因是其中仍然存在很多挑战，例如“双边下注”：

|  |
| --- |
| 如下图所示，区块链系统产生了分叉，存在两个区块A和B竞争主链时，采用权益证明的方法就是所有持币者对这两个区块投入币进行投票，从而决定哪一个区块成为最长合法链上的区块。假如有一个人，在A和B同时进行了下注。最终A区块胜出，那么他能够获得A区块相应收益，而在B区块进行投票放入的“筹码”也会被退还，这也就导致其每次都能获得收益。  由于一个人可以拥有多个账户，所以我们无法强迫一个人一次只能投向一个区块。而越有钱的人，通过“双边下注”得到的收益也就越多。 |



1. 以太坊拟采用的权益证明

以太坊中，准备采用的权益证明协议为Casper the Friendly Finality Gadget(FFG)，该协议在过渡阶段是要和POW结合使用的。

在比特币系统中，我们有提到为了防范分叉攻击，一个交易在其获得6次确认（其后跟着6个区块）后认为该区块安全。但实际上，这种安全只是概率意义上的安全，仍然可能会被拥有强大算力的用户在其前面发动分叉攻击进行回滚。

Casper协议引入一个概念：Validator(验证者)，一个用户想要成为Validator，需要上交一笔“保证金”，这笔保证金会被系统锁定(保证金使用时有一定的冷却期，不能一直重复使用)。Validator的职责是推动系统达成共识，投票决定哪一条链成为最长合法链，投票权重取决于保证金数目。

实际中，采用两次投票的方式：预投票和Commit 投票，规定每次投票结果都要获得2/3以上的验证者同意。在实际中，针对其进行了一些修改，两次投票在实际中只需要一次即可。

矿工挖矿会获得出块奖励，而验证者也会得到相应奖励。当然，为了防止验证者的不良行为，规定其被发现时要受到处罚。例如某个验证者“行政不作为”，不参与投票导致系统迟迟无法达成共识，这时扣掉部门保证金；如果某个验证者“乱作为”，给两边都进行投票，被发现后没收全部保证金。没收的保证金被销毁，从而减少系统中货币总量。验证者存在“任期”，在任期结束后，进入“等待期”，在此期间等待其他节点检举揭发是否存在不良行为，若通过等待期，则可以取回保证金并获得一定投票奖励。

**Q：这样一定能保证不被篡改吗？**

在该协议下，矿工无论算力多么强，最终投票权都不在其手中。必须在系统中，存在大量“验证者”进行了两边投票，也就是说，至少1/3（该协议规定超过2/3才有效）的验证者两侧都投票，才会导致系统被篡改。而这一旦被发现，这1/3验证者的保证金将会被没收。

|  |
| --- |
| 以太坊系统设想，随着世界推移，挖矿奖励逐渐减少而权益证明奖励逐渐增多，从而实现POW到POS的过渡，最终实现完全放弃挖矿。 |

然而权益证明仍然存在缺陷，但工作量证明已经得到了事实检验，该机制较为成熟。目前，EOS加密货币，即“柚子”，2018年上线，就是采用权益证明的共识机制，其采用的是DPOS：Delegated Proof of Stake。该协议核心思想是通过投票选21个超级节点，再由超级节点产生区块。但目前，权益证明仍然处于探索阶段。

**预挖矿(Pre-Mining)**

以太坊中采用的预挖矿的机制。这里“预挖矿”并不挖矿，而是在开发以太坊时，给开发者预留了一部分货币。以太坊的早期开发者，目前就很有钱了。而比特币并未采用这一模式，所有比特币都是通过挖矿产生的。但早期挖矿难度容易，所有中本聪本人本来就有很多币(但没花…)

和Pre-Mining对应，还有Pre-Sale，Pre-Sale指的是将预留的货币出售掉用于后续开发，类似于拉风投或众筹。目前，各类加密货币很多，存在一部分货币就在采用Pre-Sale来获取资金，如果此时买入，后续如果该货币取得成功，同样可以获得很大收益，但真正成功的货币只占少数，这就是其风险性。

**其他观点**

前面的基本观点都是基于“挖矿消耗大量电能，而这是不好的”这一观点，但也有人持有相反观点。

他们认为其所消耗的电能所占比值并不大，而且其对于环境的影响是有限的。挖矿提供了将电能转换为钱的手段，而电能本身难以传输和存储，一般来说，白天所发的电不足，晚上所发的电又多于实际需求。因此，挖矿为将多余的电脑转换为有价值的货币提供了很好的解决手段。也就是说挖矿消耗电能可以有效消耗过剩产能，带动当地经济发展。

针对于挖矿算法的其它观点，挖矿算法设计一直趋向于让大众参与，这一才是公平的。且由于参与人员的分散，算力分散，也进一步使得系统更安全。

但同样一件事物，从不同观点看就有不同的看法。也有人认为让普通计算机参与挖矿是不安全的，像比特币那样，让中心化矿池参与挖矿才是安全的。为什么呢？

因为要攻击系统，需要购入大量只能进行特定货币挖矿的矿机通过算力进行强行51%攻击，而攻击成功后，必然导致该币种的价值跳水，攻击者投入的硬件成本将会全部打水漂。而如果让通用计算机也参与挖矿，发动攻击成本便大幅度降低，目前的大型互联网公司，将其服务器聚集起来进行攻击即可，而攻击完成后这些服务器仍然可以转而运行日常业务。因此，也有人认为，在挖矿上面，ASIC矿机“一统天下”才是最安全的方式。