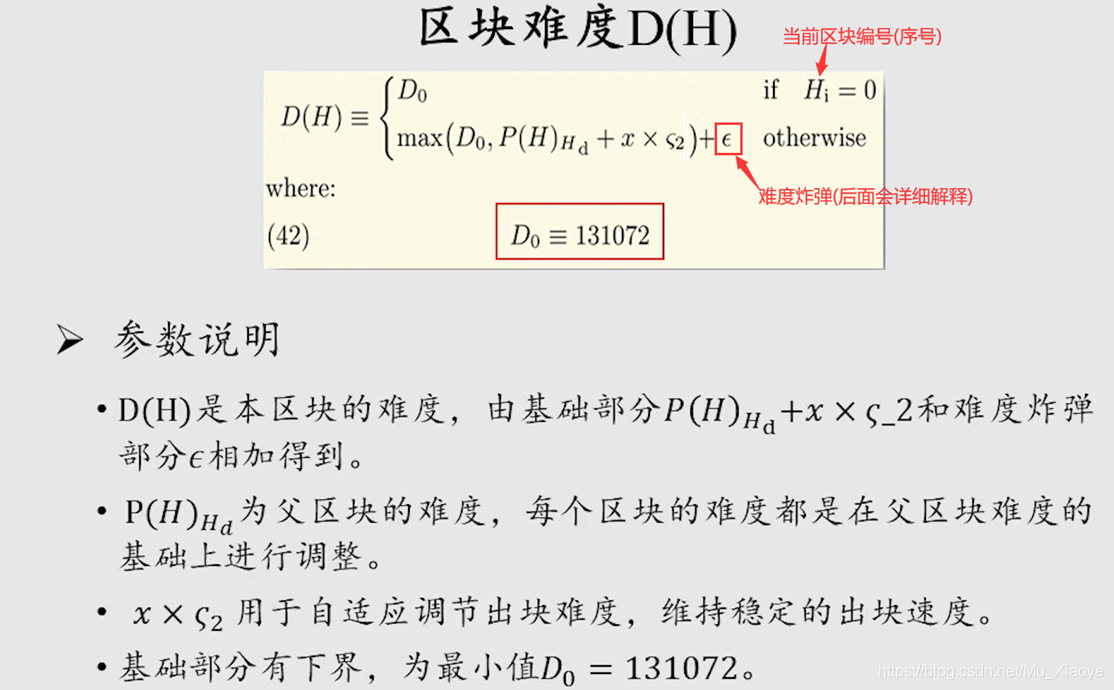
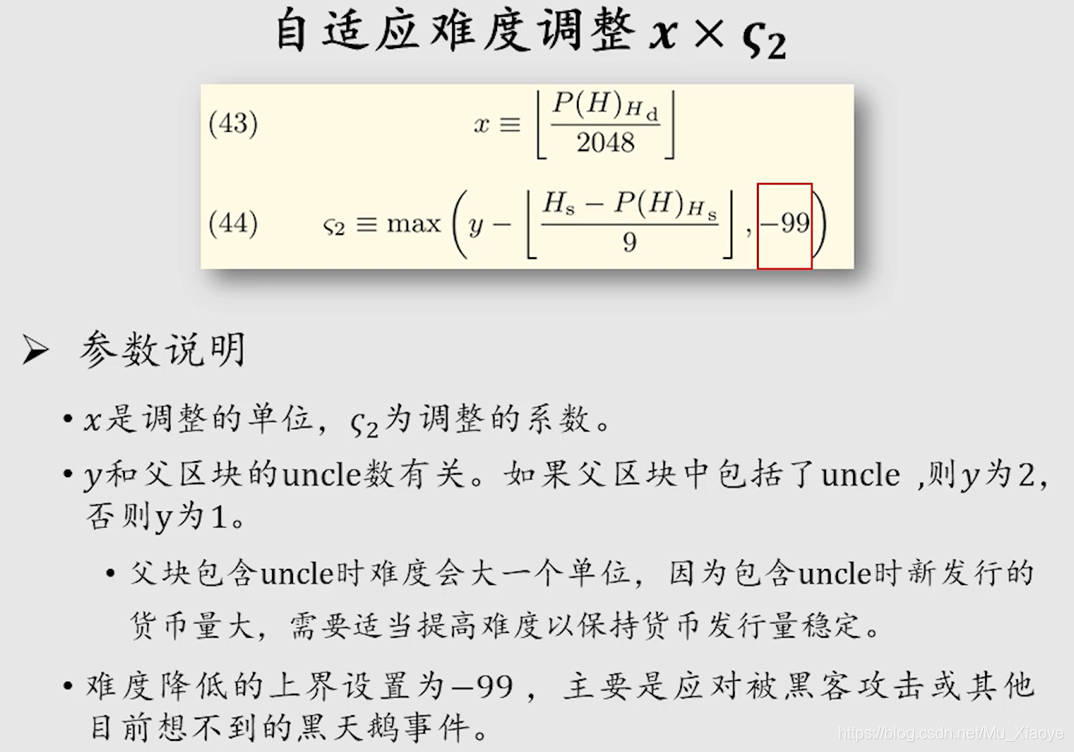
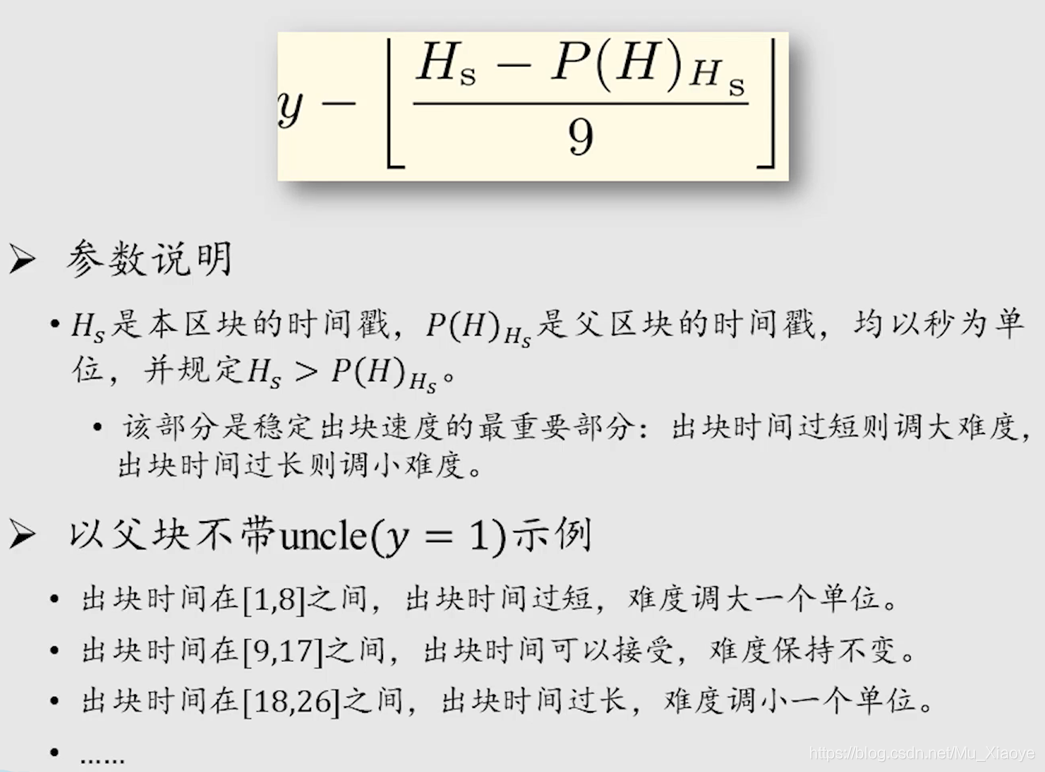
前文中介绍了比特币难度调整是每隔2016个区块调整难度，从而达到维持出块时间10min的目标。而以太坊则与之不同，每个区块都有可能会进行难度调整。以太坊难度调整较为复杂，存在多个版本，网络上存在诸多不一致，这里遵循**以代码逻辑为准**的原则，从代码中查看以太坊难度调整算法。

1. 以太坊难度调整

以太坊中区块难度调整算法如下图所示：





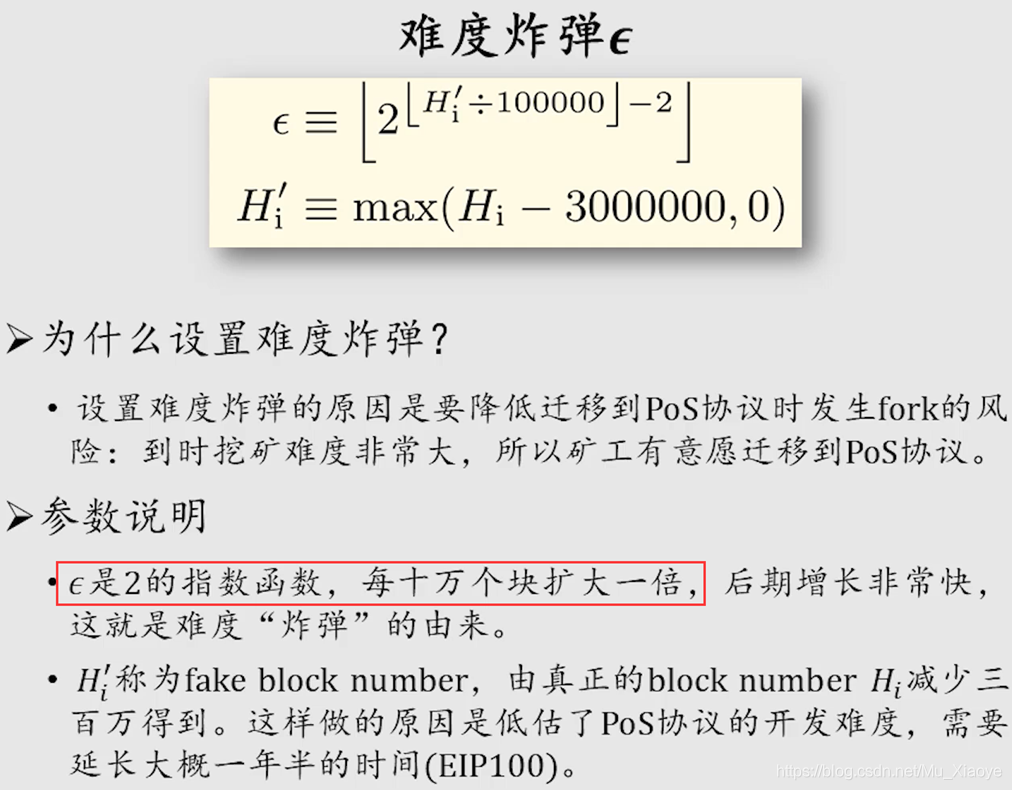


1. 难度炸弹
2. 为什么要设置难度炸弹？

根据以上以太坊难度调整算法可以看到，该算法可以很好地动态调整挖矿难度，从而保障系统整体出块时间维持在15s左右。但之前在挖矿算法的文章中有介绍到，以太坊在设计之初就计划要逐步从POW（工作量证明）转向POS（权益证明），而权益证明不需要挖矿。

从旁观者角度来看，挖矿消耗了大量电力、资金等，如果转入放弃挖矿，必然是一件好事。但从矿工的角度，花费了很大精力投入成本购买设备，突然被告知“不挖矿了”，这必然是一件很难接受的事情。而以太坊本身为一个分布式系统，其转入POS必须经过系统中大多数矿工认可才行，如果届时矿工联合起来转入POS，那么这一设计初衷就成了一江流水。

因此，以太坊在设计之初便添加了难度炸弹，**迫使矿工转入POS**。那么 如何促使矿工自愿升级软件，而非坚持POS呢？



|  |
| --- |
| 数学上，指数函数是一个很可怕的东西。我们谈论一个算法，无论其时间复杂度还是空间复杂度，只要达到了指数级别，这个算法必然难以应用于大规模计算上。指数函数在前期增长相对缓慢，但在后期呈现“指数爆炸”，而这往往是我们无法通过升级硬件所能解决的。 |

可以看到，在以太坊早期时，区块号较小，难度炸弹计算所得值较小，难度调整级别基本上通过难度调整中的自适应难度调整部分决定，而随着越来越多区块被挖出，难度炸弹的威力开始显露出来，这也就使得挖矿变得越来越难，从而迫使矿工愿意转入POS。

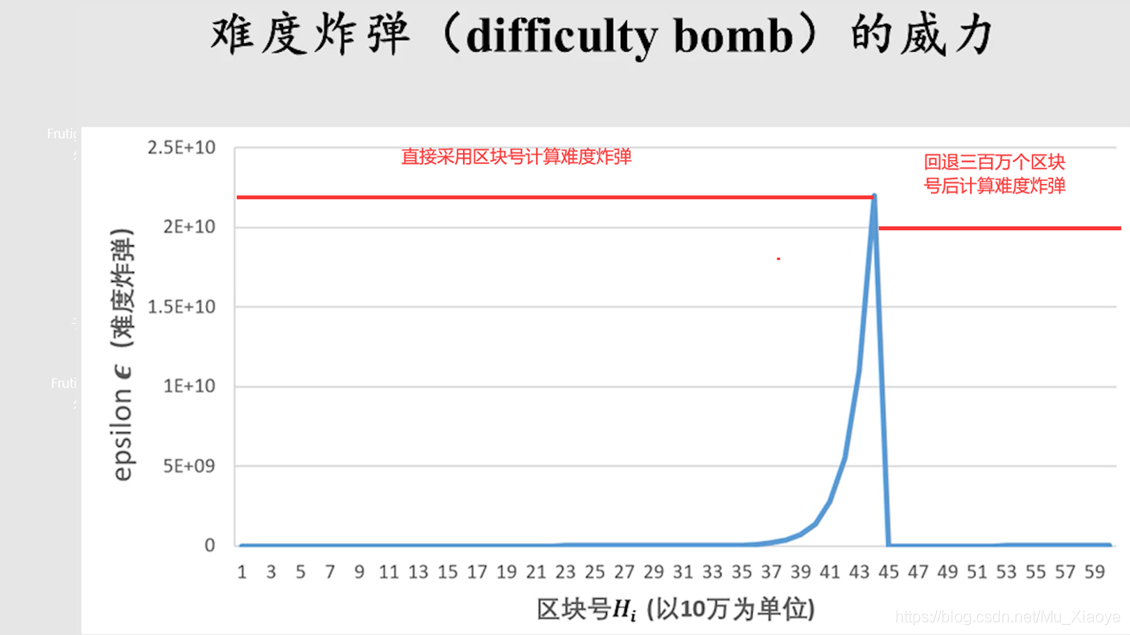
1. 难度炸弹调整

上面提到，以太坊设想是通过埋设难度炸弹迫使矿工届时愿意转入权益证明，但现实中有一句话：“理想很丰满，现实很骨感”。在实际应用中，权益证明的方式仍然并不成熟，目前以太坊共识机制仍然是POW，依然需要矿工参与挖矿维护以太坊系统的稳定。也就是说，转入POS的时间节点被一再推迟，虽然挖矿变得越来越难，系统出块时间开始逐渐变长，但矿工仍然需要继续挖矿。

在上面难度炸弹的公式中，有人应该注意到了第二项中的fake block number，该数仅仅为对当前区块编号减去了三百万，也就是相当于将区块编号回退了三百万个。那么，在前三百万个区块的时候，这个fake block number就是负数吗？

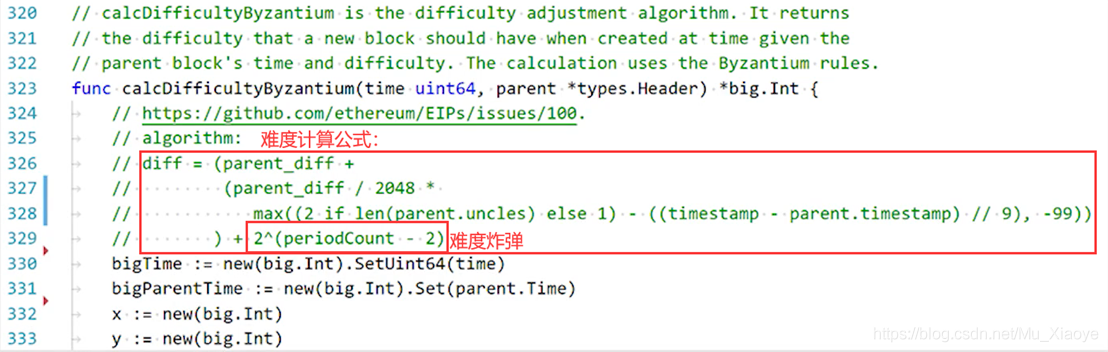
答案是否定的。实际上，在以太坊最初的设计中，并没有第二个公式。也就是说，最初就是简单地直接用区块编号除以100000。而在转入权益证明时间节点一再推迟后，以太坊系统采取了将区块编号回退三百万个区块的方法来降低挖矿难度，当然，为了保持公平，也将出块奖励从5个以太币减少到了3个以太币，这也是fake block number这一项出现的原因。

下图显示了难度调整对难度炸弹难度影响的结果：

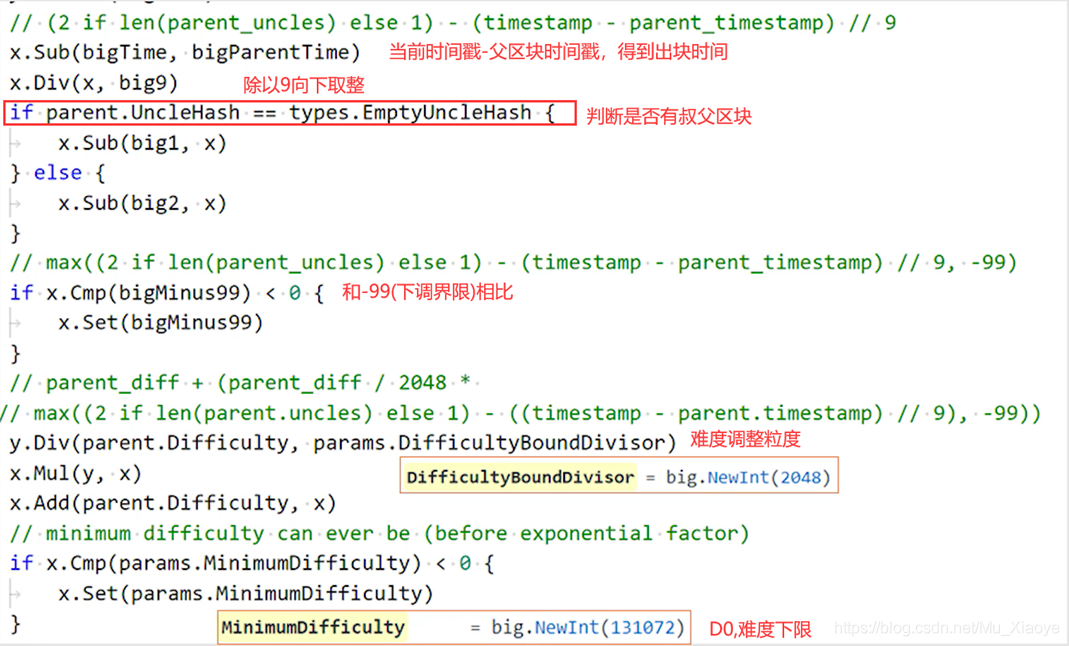


1. 具体代码实现
2. 难度计算公式

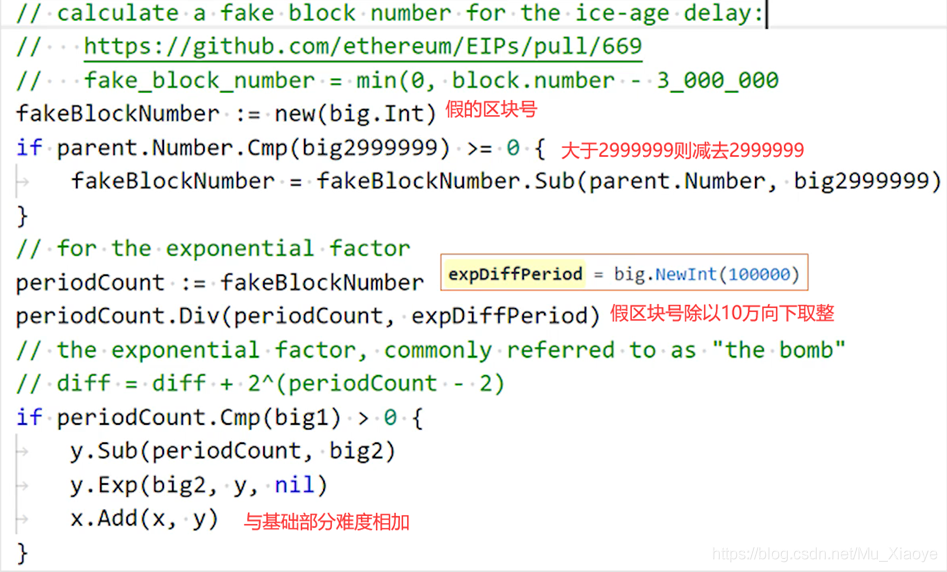
bigTime为当前区块时间戳，bigParentTime为当前区块的父区块时间戳。



1. 基础部分计算



1. 难度炸弹计算

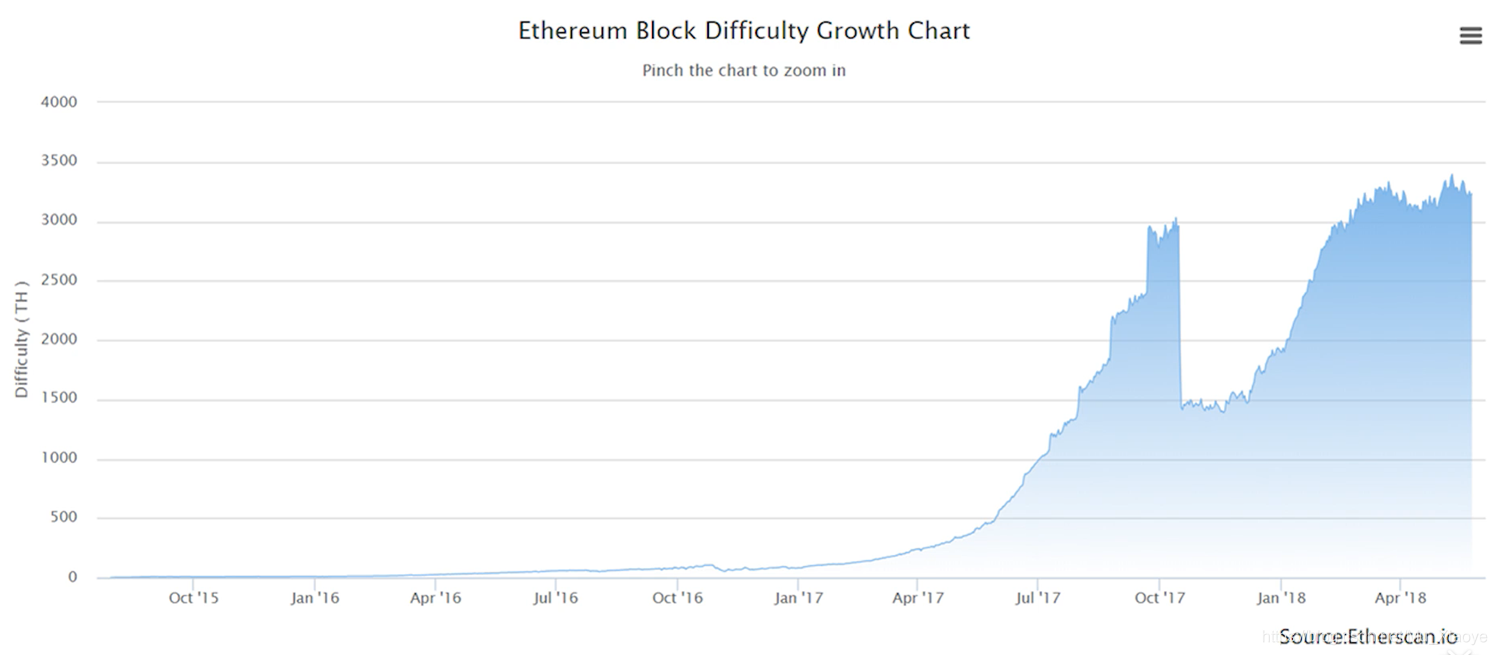


为什么不是减去3000000，而是2999999？

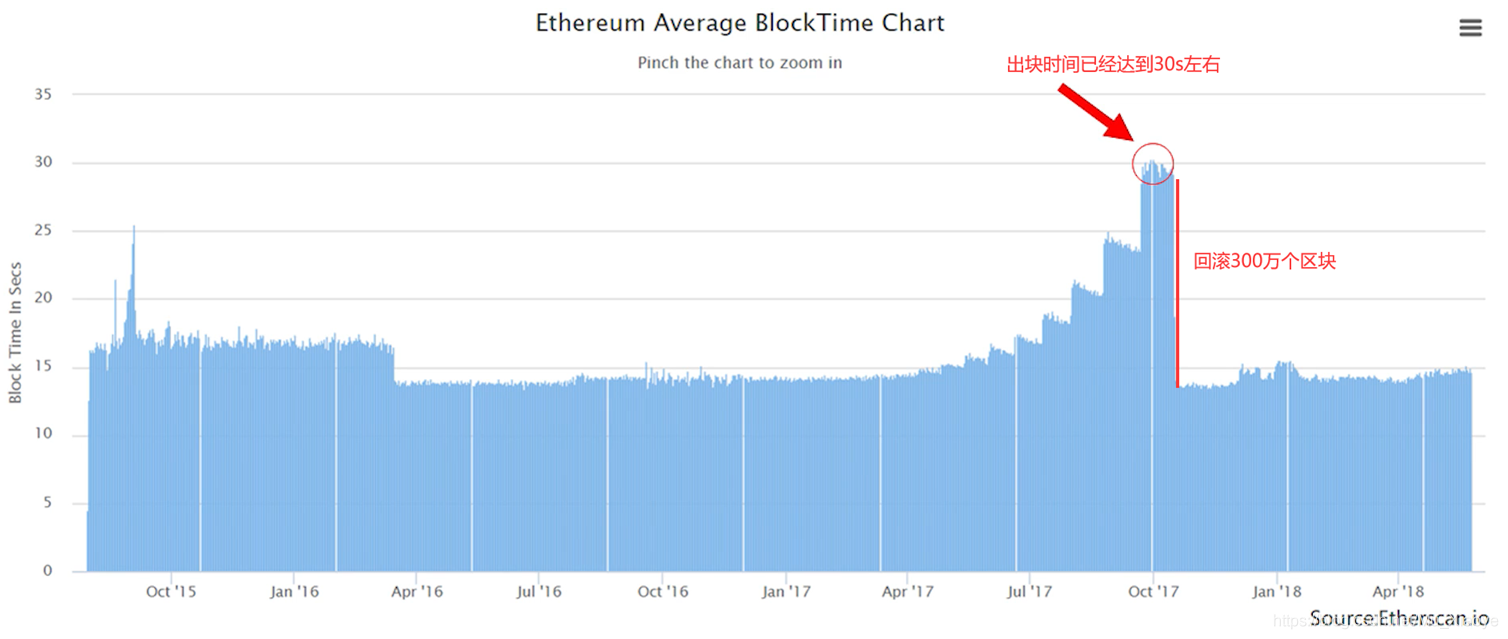
因为这里判断的父区块号，而公式中是根据当前区块来算的。

1. 以太坊实际统计数据(2018年，取自肖老师授课PPT)
2. 以太坊挖矿难度变化曲线

断崖式下跌是由于下调难度炸弹300万个区块。



1. 以太坊出块时间变化曲线图



1. 两个真实区块信息

difficulty为当前区块难度，total difficulty为当前区块链上所有区块难度相加。

可见，最长合法链也就等同于最难合法链（难度最大合法链）。

