

20 ETH挖矿难度调整算法

以太坊中的平均出块时间是15秒，每个区块都有可能调整难度，要比比特币的难度调整复杂的多。

区块难度D(H)

$$D(H) \equiv \begin{cases} D_0 & \text{if } H_i = 0 \\ \max(D_0, P(H)_{H_d} + x \times \varsigma_2) + \epsilon & \text{otherwise} \end{cases}$$

where:

$$(42) \quad D_0 \equiv 131072$$

➤ 参数说明

- $D(H)$ 是本区块的难度，由基础部分 $P(H)_{H_d}+x \times \varsigma_2$ 和难度炸弹部分 ϵ 相加得到。
- $P(H)_{H_d}$ 为父区块的难度，每个区块的难度都是在父区块难度的基础上进行调整。

自适应难度调整 $x \times \varsigma_2$

$$(43) \quad x \equiv \left\lfloor \frac{P(H)_{H_d}}{2048} \right\rfloor$$

$$(44) \quad \varsigma_2 \equiv \max \left(y - \left\lfloor \frac{H_s - P(H)_{H_s}}{9} \right\rfloor, -99 \right)$$

➤ 参数说明

- x 是调整的单位， ς_2 为调整的系数。

自适应难度调整 $x \times \zeta_2$

$$(43) \quad x \equiv \left\lfloor \frac{P(H)_{H_d}}{2048} \right\rfloor$$

$$(44) \quad \zeta_2 \equiv \max \left(y - \left\lfloor \frac{H_s - P(H)_{H_s}}{9} \right\rfloor, -99 \right)$$

➤ 参数说明

- x 是调整的单位， ζ_2 为调整的系数。
- y 和父区块的 uncle 数有关。如果父区块中包括了 uncle，则 y 为 2，否则 y 为 1。
 - 父块包含 uncle 时难度会大一个单位，因为包含 uncle 时新发行的货币量大，需要适当提高难度以保持货币发行量稳定。

-99 是为了限制一次性下调的太多，为了避免一些意想不到的事情发生。

$$y = \left\lfloor \frac{H_s - P(H)_{H_s}}{9} \right\rfloor$$

➤ 参数说明

- H_s 是本区块的时间戳， $P(H)_{H_s}$ 是父区块的时间戳，均以秒为单位，并规定 $H_s > P(H)_{H_s}$ 。
 - 该部分是稳定出块速度的最重要部分：出块时间过短则调大难度，出块时间过长则调小难度。

➤ 以父块不带uncle($y = 1$)示例

- 出块时间在[1,8]之间，出块时间过短，难度调大一个单位。
- 出块时间在[9,17]之间，出块时间可以接受，难度保持不变。
- 出块时间在[18,26]之间，出块时间过长，难度调小一个单位。
-

难度炸弹 ϵ

$$\epsilon \equiv \left\lfloor 2^{\lfloor H'_i \div 100000 \rfloor - 2} \right\rfloor$$
$$H'_i \equiv \max(H_i - 3000000, 0)$$

➤为什么设置难度炸弹？

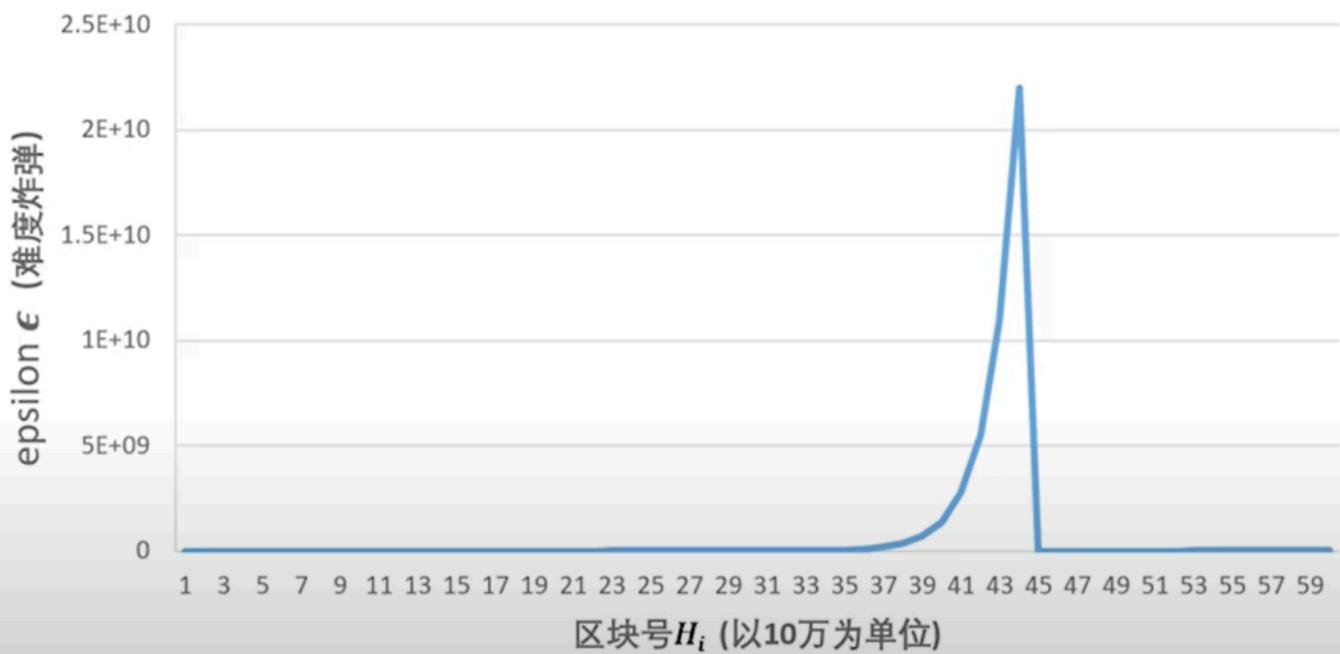
- 设置难度炸弹的原因是要降低迁移到PoS协议时发生fork的风险：到时挖矿难度非常大，所以矿工有意愿迁移到PoS协议。

➤参数说明

- ϵ 是2的指数函数，每十万个块扩大一倍，后期增长非常快，这就是难度“炸弹”的由来。
- H'_i 称为fake block number，由真正的block number H_i 减少三百万得到。这样做的原因是低估了PoS协议的开发难度，需要延长大概一年半的时间(EIP100)。

难度炸弹的设置是为了防止转换成权益证明之后，一些在挖矿设备上花费了很多金钱的矿工，可能就不愿意调整成权益证明，而是坚持工作量证明。

难度炸弹（difficulty bomb）的威力



以太坊发展的四个阶段

Frontier

Homestead

Metropolis

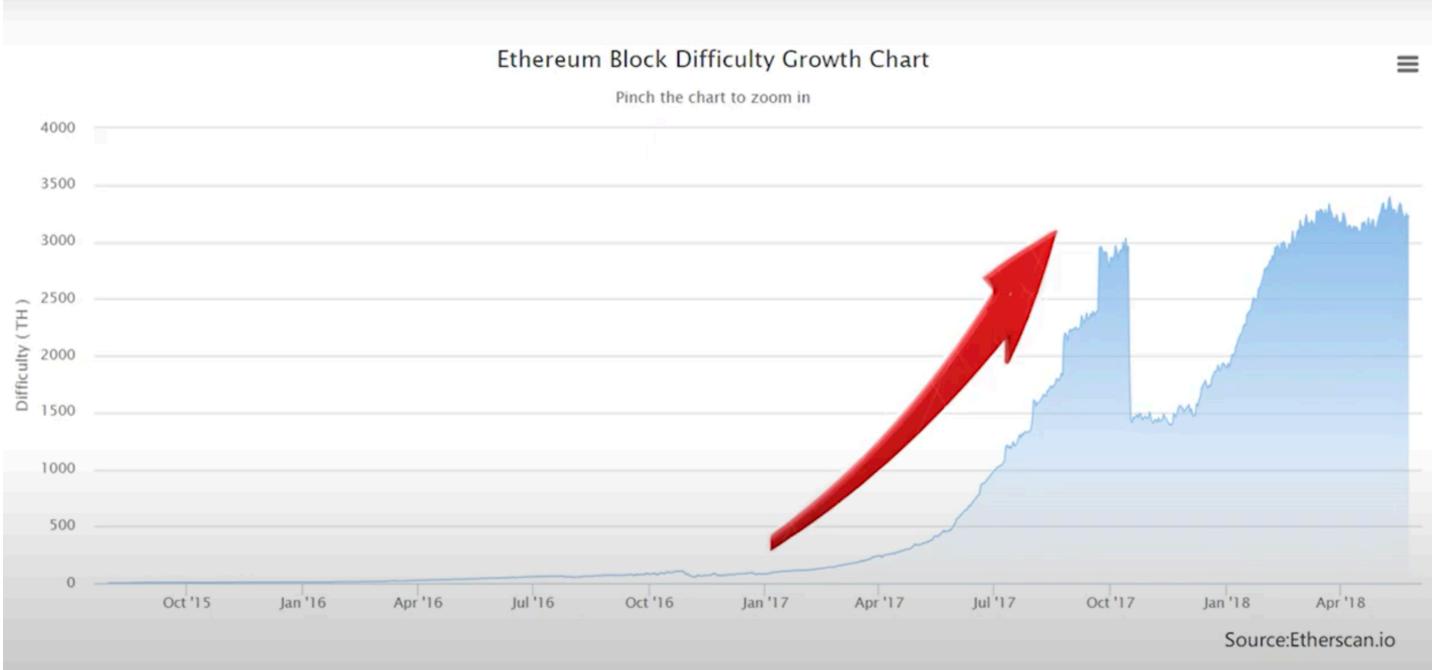
Byzantium

Constantinople

Serenity

➤ 说明

- Metropolis又分为Byzantium和Constantinople两个子阶段。
- 难度炸弹的回调发生在Byzantium这个子阶段，在EIP（Ethereum Improvement Proposal）中决定，同时把block reward从5个ETH降为3个ETH。



Ethereum Average BlockTime Chart

≡

Pinch the chart to zoom in

